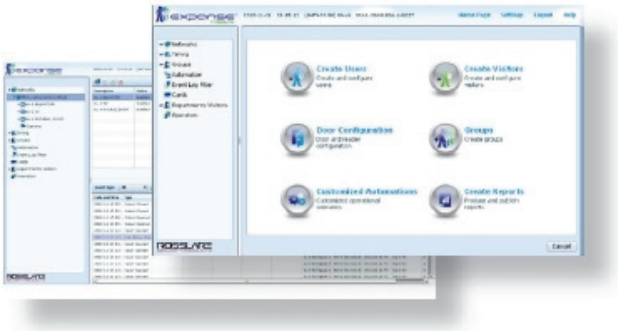
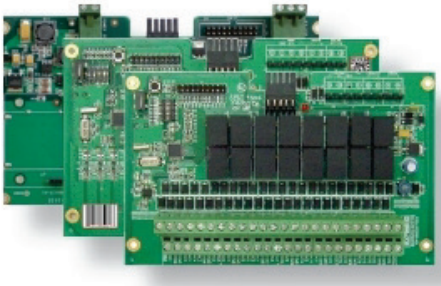
2012
March

# ExpansE

## Distributed Access Control System

Software Manual





ROSSLARE
SECURITY PRODUCTS

**Copyright © 2012 by Rosslare. All rights reserved.**

This manual and the information contained herein are proprietary to REL, RSP Inc. and/or their related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

# Table of Contents

**1. Introduction ..... 16**
1.1 System Overview ..... 16
1.2 Features ..... 17
1.3 ExpansE Web Application ..... 17
1.3.1 Configurable Links ..... 17
1.4 ExClouds Reports Production Software ..... 17
1.4.1 ExClouds Structure ..... 17
**2. Technical Specifications ..... 18**
2.1 EXP-1032 Networked Controller ..... 18
2.2 EXP-2024 Dual Reader Door Unit ..... 18
2.3 EXP-2016 16-Relay Elevator Control Unit ..... 19
2.4 EXP-2088 8-Input/Output Interface ..... 20
2.5 EXP-3002 2-Channel Video Board ..... 20
2.6 System Environmental Characteristics ..... 21
**3. ExpansE Architecture ..... 22**
3.1 Central versus Distributed Topology ..... 22
3.2 ExpansE Distributed Access Control ..... 24
3.3 ExpansE Mounting Options ..... 25
3.3.1 ME-01 Single Board Self-Powered Metal Enclosure ..... 25
3.3.2 ME-12 Single Board Self-Powered Plastic Enclosure ..... 25
3.3.3 ME-14 Compact Single Board Self-Powered Enclosure ..... 26
3.3.4 ME-00 9-Board Tray Cabinet Housing ..... 27
3.4 ExpansE Hardware Units ..... 27
3.4.1 EXP-1032 ExpansE Networked Controller ..... 28
3.4.2 EXP-2024 Dual Reader Door Unit ..... 28
3.4.3 EXP-2016 16-Relay Elevator Control Unit ..... 29
3.4.4 EXP-2088 8-Input/Output Interface Unit ..... 29
3.4.5 EXP-3002 2-Channel Video Board ..... 30

3.5 Reports Production and Backup Software ..... 30
3.6 Card Readers and Keypads ..... 30
**4. Hardware Installation ..... 31**
4.1 Wiring Instructions ..... 31
4.1.1 EXP-1032 ExpansE Networked Controller ..... 31
4.1.2 EXP-2024 Dual Reader Door Unit ..... 32
4.1.3 EXP-2016 16-Relay Elevator Control Unit ..... 35
4.1.4 EXP-2088 – 8-Input/Output Interface ..... 36
4.2 ME-00 9-Board Tray Cabinet Housing Wiring ..... 37
4.3 Power Supply ..... 38
4.4 RS-485 Daisy Chain ..... 39
4.5 Inputs and Outputs ..... 39
4.5.1 Input Types ..... 39
4.5.2 Inputs Description ..... 43
4.5.3 Output Description ..... 43
4.6 Output Wiring ..... 44
4.7 Mounting ..... 46
4.7.1 ME-01 Single Board Self-Powered Metal Enclosure ..... 46
4.7.2 ME-12 Single Board Self-Powered Plastic Enclosure ..... 47
4.7.3 ME-14 Compact Single Board Self-Powered Enclosure ..... 51
4.7.4 ME-00 9-Board Tray Cabinet Housing ..... 52
4.8 DIP Switch Configuration ..... 53
4.8.1 Network Addressing ..... 54
4.8.2 Tamper Enabling ..... 56
**5. Communications ..... 57**
**6. The ExpansE Web Application ..... 58**
6.1 Initial PC Configuration ..... 58
6.2 Initial Access and Network Settings ..... 63
6.3 The ExpansE Main Window ..... 66
6.4 Tree View ..... 67
6.4.1 Networks ..... 67
6.4.2 Cameras ..... 67

6.4.3 Maps ..... 67
6.4.4 Timing ..... 67
6.4.5 Groups ..... 67
6.4.6 Automation ..... 67
6.4.7 Event Log Filter ..... 67
6.4.8 Cards ..... 68
6.4.9 Departments and Visitors ..... 68
6.4.10 Operators ..... 68
6.5 Toolbar ..... 68
6.5.1 General Icons ..... 68
6.5.2 Event Type Icon ..... 69
6.6 Menu Bar ..... 69
6.6.1 Home Page ..... 69
6.6.2 Tools ..... 69
6.6.3 Logout ..... 70
6.6.4 Help Menu ..... 70
6.7 Event Log ..... 70
**7. How to Set Up a Site ..... 71**
7.1 Setting a Controller (MU) ..... 71
7.2 Configuring Doors ..... 73
7.3 Setting a 16-Relay Elevator Control Unit ..... 75
7.4 Configuring Readers ..... 76
7.5 Configuring Inputs and Outputs ..... 77
7.6 Adding Cameras ..... 79
7.7 Adding Active Maps ..... 79
7.8 Adding Time Zones and Holidays ..... 84
7.9 Adding Access Groups ..... 86
7.10 Adding Input Groups ..... 87
7.11 Adding Output Groups ..... 88
7.12 Adding Elevator Groups ..... 89
7.13 Adding Automation ..... 90
7.14 Adding Cards ..... 91

7.15 Adding Departments and Users ..... 92
7.16 Adding Visitors ..... 96
7.17 Setting Event Log Filters ..... 100
7.18 Defining Operators ..... 101
**8. Configuration Wizards ..... 103**
8.1 Customized Automation Wizard ..... 103
8.2 Create Users Wizard ..... 106
8.3 Create Visitors Wizard ..... 112
8.4 Doors Wizard ..... 118
8.5 Groups Wizard ..... 122
8.5.1 Access Groups ..... 123
8.5.2 Input Groups ..... 125
8.5.3 Output Groups ..... 127
8.5.4 Elevators Groups ..... 129
**9. Manual Operation ..... 131**
9.1 Manual Door Control ..... 131
9.2 Manual Reader Control ..... 132
9.3 Manual Output Control ..... 132
**10. ExClouds ..... 134**
10.1 ExClouds Application ..... 134
10.1.1 Minimum Requirements ..... 134
10.1.2 ExClouds Application Installation ..... 134
10.1.3 ExClouds Setup ..... 136
10.1.4 Tools Menu ..... 138
10.2 ExClouds Web Server ..... 138
10.2.1 Minimum Requirements ..... 138
10.2.2 Software Prerequisite ..... 139
10.2.3 ExClouds Web Server Installation ..... 139
10.2.4 Viewing the Camera Stream ..... 143
10.2.5 Editing Camera Properties ..... 144
10.2.6 Recording and Configuring Camera Streams ..... 145
10.2.7 Downloading Camera Streams ..... 149

**11. Reports Wizard ..... 150**
11.1 Initiating the Report Wizard ..... 150
11.2 Creating Roll Call Reader Report ..... 151
11.3 Creating Last Known Position Report ..... 152
11.4 Creating System Report ..... 153
11.5 Creating an Attendance Report..... 155
**12. Firmware Update ..... 159**
**A. Example of Wiring an Elevator Unit ..... 162**
**Limited Warranty ..... 164**

# List of Figures

Figure 1: Central versus Distributed Architectures ..... 23
Figure 2: Sample of ExpansE Configuration..... 24
Figure 3: ME-01 Single-Board Self-Powered Metal Enclosure..... 25
Figure 4: ME-12 Single-Board Self-Powered Plastic Enclosure ..... 26
Figure 5: ME-14 Compact Single-Board Self-Powered Enclosure..... 26
Figure 6: ME-00 9-Board Tray Cabinet Housing ..... 27
Figure 7: EXP-1032 ExpansE Networked Controller ..... 28
Figure 8: EXP-2024 Dual Reader Door Unit ..... 28
Figure 9: EXP-2016 16-Relay Elevator Control Unit ..... 29
Figure 10: EXP-2088 8-Input/Output Interface Unit..... 29
Figure 11: EXP-3002 2-Channel Video Board ..... 30
Figure 12: EXP-1032 ExpansE Networked Controller Wiring..... 31
Figure 13: EXP-2024 Dual Reader Door Wiring ..... 33
Figure 14: EXP- 2024 Dual Reader Door Unit Wiring Details..... 34
Figure 15: EXP-2016 16-Relay Elevator Control Unit Wiring ..... 35
Figure 16: EXP-2016 16-Relay Outputs Elevator Control Unit Wiring ..... 36
Figure 17: EXP-2088 8-Input/Output Interface Wiring ..... 36
Figure 18: EXP-2088 8-Input/Output Interface Detailed Wiring..... 37
Figure 19: ME-00 9-Board Tray Cabinet Housing Wiring ..... 38
Figure 20: Wiring the Power Supply..... 39
Figure 21: Normally Open Input Connection..... 40
Figure 22: Normally Closed Input Connection..... 41
Figure 23: Normally Open Supervised Input (Single Resistor)..... 41
Figure 24: Normally Open Supervised Input (Double Resistor)..... 42
Figure 25: Normally Closed Supervised Input (Single Resistor)..... 42
Figure 26: Normally Closed Supervised Input (Double Resistor)..... 43
Figure 27: Power Enabled Output Wiring..... 45
Figure 28: Non-Power Output Wiring ..... 45
Figure 29: ME-01 Mounting Template ..... 46
Figure 30: ME-01 Wall Mounting ..... 47
Figure 31: ME-01 Unit Mounting and In-Box Connections..... 47
Figure 32: ME-12 Mounting Template ..... 49
Figure 33: ME-12 Wall Mounting ..... 50

Figure 34: ME-12 Unit Mounting, In-Box Connections and wiring ..... 50
Figure 35: ME-14 Mounting Template ..... 51
Figure 36: ME-14 Assembly ..... 51
Figure 37: ME-00 Mounting Template ..... 52
Figure 38: ME-00 Units Placement ..... 53
Figure 39: ME-00 Wiring Threads ..... 53
Figure 40: DIP Switch ..... 54
Figure 41: Internal Network Address DIP Switch Setting ..... 54
Figure 42: Tamper DIP Switch Setting ..... 56
Table 3: DIP Switch Settings for Tamper Enabling ..... 56
Figure 43: Windows XP – Control Panel ..... 58
Figure 44: Windows XP – Network Connections ..... 59
Figure 45: Windows XP – Local Area Connection Status Window ..... 59
Figure 46: Windows XP – Local Area Connection Properties Windows ..... 60
Figure 47: Windows XP – Internet Protocol (TCP/IP) Properties Window ..... 60
Figure 48: Windows Vista/7 – Network and Sharing Center ..... 61
Figure 49: Windows Vista/7 – Local Area Connection Status Window ..... 62
Figure 50: Windows Vista/7 – Local Area Connection Properties Window. 62
Figure 51: Windows XP – Internet Protocol (TCP/IP) Properties Window ..... 63
Figure 52: ExpansE Web Application Login Screen ..... 64
Figure 53: ExpansE Web Application Homepage ..... 64
Figure 54: System Settings – General Tab ..... 65
Figure 55: System Settings – Date and Time Tab ..... 65
Figure 56: ExpansE Web Application Main Screen ..... 66
Figure 57: Tools Menu ..... 69
Figure 58: Search Option ..... 69
Figure 59: Search Results Tab ..... 70
Figure 60: ExpansE Web Application About Screen ..... 70
Figure 61: ExpansE Web Application Networks Screen ..... 72
Figure 62: Network Properties Window ..... 72
Figure 63: Networks Screen with Connected EUs ..... 73
Figure 64: Door Controller Properties Window ..... 74
Figure 65: Elevator Control EU Window ..... 75
Figure 66: Reader Properties Window ..... 76
Figure 67: Input Properties Window ..... 78
Figure 68: Output Properties Window ..... 78

## List of Figures

Figure 69: Add Video Appliance Window ..... 79
Figure 70: Map Management Screen ..... 80
Figure 71: Map Properties Window ..... 80
Figure 72: Select Image Window ..... 81
Figure 73: Select Networks Window ..... 81
Figure 74: Map Properties Window with Devices ..... 82
Figure 75: Map Design Mode ..... 83
Figure 76: Map Run Mode ..... 83
Figure 77: Timing Window ..... 84
Figure 78: Add Time Zone Window ..... 84
Figure 79: Time Zone Window ..... 85
Figure 80: Holiday Properties Window ..... 85
Figure 81: Access Group Window ..... 86
Figure 82: Access Group Properties Window ..... 86
Figure 83: Add Access Group Window with Associated Readers ..... 87
Figure 84: Add Input Group Window ..... 88
Figure 85: Output Group Window ..... 89
Figure 86: Output Group Window ..... 90
Figure 87: Automation Properties Window ..... 91
Figure 88: Add Cards Window ..... 92
Figure 89: Departments/Users/Visitors Window ..... 93
Figure 90: Department Dialog ..... 93
Figure 91: User Properties Window – General Tab ..... 94
Figure 92: User Properties Window – Details Tab ..... 95
Figure 93: User Properties Window – Codes Tab ..... 96
Figure 94: User Properties Visitor Window – General Tab ..... 97
Figure 95: User Properties Visitor Window – Details Tab ..... 98
Figure 96: User Properties Visitor Window – Codes Tab ..... 99
Figure 97: User Properties Visitor Window – Visitor Tab ..... 100
Figure 98: Even Filter Window ..... 101
Figure 99: Operator Properties Window – New ..... 102
Figure 100: ExpansE Wizards on Home Page ..... 103
Figure 101: Customized Automation Wizard Icon ..... 103
Figure 102: Customized Automation Wizard Welcome Page ..... 104
Figure 103: Customized Automation Wizard Source Page **Error! Bookmark not defined.**
Figure 104: Customized Automation Wizard Destination Page **Error! Bookmark not defined.**

Figure 105: Automation Wizard Complete Page ..... 106
Figure 106: Automation Wizard – Report Window..... 106
Figure 107: Create User Wizard Icon..... 107
Figure 108: User Wizard Welcome Page ..... 107
Figure 109: User Wizard – User Details Page ..... 108
Figure 110: User Wizard – Validity Page..... 108
Figure 111: User Wizard – Automation Page..... 109
Figure 112: User Wizard – Access Rights Page ..... 109
Figure 113: User Wizard – Card Association Page ..... 110
Figure 114: User Wizard – PIN Code Association Page..... 111
Figure 115: User Wizard Complete Page..... 111
Figure 116: User Wizard – User Report Window ..... 112
Figure 117: Create Visitor Wizard Icon..... 112
Figure 118: Visitor Wizard Welcome Page..... 113
Figure 119: Visitor Wizard – Visitor's Details Page ..... 113
Figure 120: Visitor Wizard – Validity Page ..... 114
Figure 121: Visitor Wizard – Automation Page..... 114
Figure 122: Visitor Wizard – Access Rights Page..... 115
Figure 123: Visitor Wizard – Card Association Page ..... 115
Figure 124: Visitor Wizard – PIN code association Page ..... 116
Figure 125: Visitor Wizard – Host Association Page..... 117
Figure 126: Visitor Wizard Complete Page ..... 117
Figure 127: Doors Wizard Icon ..... 118
Figure 128: Doors Wizard – Welcome Page ..... 118
Figure 129: Doors Wizard – Door Selection Page ..... 119
Figure 130: Doors Wizard – Door Details Page ..... 119
Figure 131: Doors Wizard – Door Timers Page ..... 120
Figure 132: Doors Wizard – Reader Properties Page ..... 121
Figure 133: Door Wizard – Complete Page ..... 122
Figure 134: Door Wizard – Report Window ..... 122
Figure 135: Groups Wizard Icon ..... 123
Figure 136: Groups Wizard Welcome Page ..... 123
Figure 137: Groups Wizard – Access Group Definition Page..... 124
Figure 138: Groups Wizard Complete Page ..... 124
Figure 139: Groups Wizard Icon ..... 125
Figure 140: Groups Wizard Welcome Page ..... 125

## List of Figures

Figure 141: Groups Wizard – Input Group Definition Page ..... 126
Figure 142: Groups Wizard Complete Page ..... 126
Figure 143: Groups Wizard Icon ..... 127
Figure 144: Groups Wizard Welcome Page ..... 127
Figure 145: Groups Wizard – Output Group Definition Page ..... 128
Figure 146: Groups Wizard Complete Page ..... 128
Figure 147: Groups Wizard Icon ..... 129
Figure 148: Groups Wizard Welcome Page ..... 129
Figure 149: Groups Wizard – Output Group Definition Page ..... 130
Figure 150: Groups Wizard Complete Page ..... 130
Figure 151: Door Manual Operation Window ..... 131
Figure 152: Door Manual Operation Window ..... 132
Figure 153: Door Manual Operation Window ..... 133
Figure 154: ExClouds – Disk Space Screen ..... 135
Figure 155: ExClouds – Login Screen ..... 136
Figure 156: ExClouds – Main Window ..... 136
Figure 157: ExClouds – Option Window ..... 137
Figure 158: ExClouds – Database Option Window ..... 137
Figure 159: VMware Player Window ..... 140
Figure 160: ExClouds icon in VMware Player Window ..... 141
Figure 161: ExClouds – WMware Player Window ..... 141
Figure 162: ExClouds Virtual Machine Window ..... 142
Figure 163: Setting Server IP Address ..... 143
Figure 164: Live Camera Stream ..... 144
Figure 165: Buttons to Change Stream View ..... 144
Figure 166: Video Appliance Properties Window ..... 145
Figure 167: Video Properties – Live Tab ..... 146
Figure 168: Video Properties – Display Tab ..... 146
Figure 169: Video Properties – Text Overlay Tab ..... 147
Figure 170: Video Properties – Settings Tab ..... 148
Figure 171: Video Properties – Audio Tab ..... 148
Figure 172: Records Propeties Window ..... 149
Figure 173: ExClouds – Login Screen ..... 150
Figure 174: ExClouds – Main Window with Report Option Open ..... 151
Figure 175: Roll Call Readers Wizard – Parameter Screen ..... 151
Figure 176: Roll Call Readers Wizard – Report Design Template Screen ..... 152

Figure 177: System Report Wizard – Device Selection Screen ..... 153
Figure 178: System Report Wizard – Select Event Type Screen..... 153
Figure 179: System Report Wizard – Network & Controller Selection..... 154
Figure 180: System Report Wizard – Producing Period Screen ..... 154
Figure 181: System Report Wizard – Report Save Option Screen ..... 155
Figure 182: Attendance Report Wizard – User Selection Screen..... 156
Figure 183: Attendance Report Wizard – Reader Selection Screen..... 156
Figure 184: Attendance Report Wizard – T&A Options Screen..... 157
Figure 185: Attendance Report Wizard – Producing Period Screen ..... 157
Figure 186: Attendance Report Wizard – Report Save Option Screen ..... 158
Figure 187: Controller Firmware Update Window..... 159
Figure 188: USB Stick Files for Firmware Update ..... 160
Figure 189: Selecting EU to Update Firmware ..... 160
Figure 190: Firmware Update Progress..... 161
Figure 191: Wiring Diagram of 4-Floor Elevator to EXP-2016 ..... 162
Figure 192: Connection Diagram of Four 64-Floor Elevators..... 163

# List of Tables

Table 1: EXP- 2024 Dual Reader Door Unit Wiring Details ..... 34
Table 2: Available DIP Switch Settings..... 54
Table 3: DIP Switch Settings for Tamper Enabling ..... 56

# Notice and Disclaimer

This manual's sole purpose is to assist installers and/or users in the safe and efficient installation and usage of the system and/or product, and/or software described herein.

**BEFORE ATTEMPTING TO INSTALL AND/OR USE THE SYSTEM, THE INSTALLER AND THE USER MUST READ THIS MANUAL AND BECOME FAMILIAR WITH ALL SAFETY REQUIREMENTS AND OPERATING PROCEDURES.**

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system and/or product, if applicable, is subject to the terms of the license provided as part of the purchase documents.
- REL, RSP Inc. and/or their related companies and/or subsidiaries' (hereafter: "ROSSLARE") exclusive warranty and liability is limited to the warranty and liability statement provided in an appendix at the end of this document.
- This manual describes the maximum configuration of the system with the maximum number of functions, including future options. Therefore, not all functions described in this manual may be available in the specific system and/or product configuration you purchased.
- Incorrect operation or installation, or failure of the user to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text, images and graphics contained in the manual are for the purpose of illustration and reference only.
- In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).
- All graphics in this manual are for reference only, some deviation between the image(s) and the actual product may occur.
- All wiring diagrams are intended for reference only, the photograph or graphic of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

# 1. Introduction

The ExpansE access control system is a state-of-the-art networked access control system with a web based management and control application.

The ExpansE system consists of the following components:

- EXP-1032 – ExpansE Networked Controller with on-board web-based application
- EXP-2024 – Dual Reader Door Unit
- EXP-2016 – 16-Relay Elevator Control Unit
- EXP-2088 – 8-Input/Output Interface Unit

## 1.1 System Overview

The ExpansE system's control panel does not include any on-board terminals, but instead holds a powerful processing unit as well as high-capacity network communication capabilities, which allows TCP/IP network communication via its on-board TCP/IP interface.

The system components provide all of the necessary door connections such as reader ports, lock outputs and signaling inputs, as well additional inputs and outputs for various access control applications.

Due to the component structure of the system, the various components may be installed in many variations and topologies according to the specific needs of the installation site.

The platform, since not dedicated and limited to enclosed number of doors, can be used for further processing and applications such as security, automation and others.

Targeted for the medium to large installations, this topology brings forth a solution benefiting from:

- Significantly higher capacities
- Flexible installation

  Pure processing central units, not limited by physical limitations, such as a maximum number of onboard readers, make it highly flexible for various applications, both for the initial layout and for future additions, such as door interfaces with various formats, IO interfaces and smart management, security management, elevator control, native support for video interfaces etc.

  This type of layout also supports easy future upgrading as only firmware upgrades are required.
- The EXPANSE IP also includes on-board support for communications across a TCP/IP network.

## 1.2 Features

The ExpansE is a powerful and adaptable access control solution with a wide range of features.

- Up to 2,048 Main Units connected via Ethernet
- Each Main Unit can have up to 32 End Units and up to 32 doors (IN/OUT) or 64 readers.
- Each Main Unit can have up to 256 inputs and 512 outputs
- Panel configuration DIP switch
- 128,000 users per Main Unit
- 100,000 history event log per Main Unit
- 512 multi segmented Time Zones and 128 Holidays dates
- RS-232 and RS-485 serial communication
- Ethernet and USB communication ports

## 1.3 ExpansE Web Application

The ExpansE system utilizes an embedded web based management and supervision application, which controls up to 2048 Main Units (MUs) (EXP-1032 ExpansE Networked Controller), by creating a Master/Slave configuration of all available MUs within the network, each with their associated secondary units, referred to as End Units (EUs).

### 1.3.1 Configurable Links

The system's configurable links model makes it possible to trigger any chosen output such as triggering an alarm siren, based on a signal from a selected input. This allows easy integration with other systems such as intruder alarms and CCTV systems.

ExpansE can also define a selected set of operations (defined in configurable links) when a panel registers a specified user or group of users.

## 1.4 ExClouds Reports Production Software

The ExClouds software application is used to produce custom designed reports and to manage all the reports available in the system. See Chapter 11.

In addition ExClouds has extensive backup abilities. See Chapter 10.

### 1.4.1 ExClouds Structure

ExClouds PC software operates through a dedicated computer, which communicates with the ExpansE MU.

# 2. Technical Specifications

## 2.1 EXP-1032 Networked Controller

| Electrical Characteristics | |
|---|---|
| **Operating Voltage** | 12–16 VDC 1.5 A<br>from external DC input connector |
| **Maximum Input Current** | Standby: 150 mA @ 12 V<br>Maximum: 1200 mA @ 12 V<br>(Not including attached devices) |
| **Visual Indicators** | Power LED<br>TCP/IP Speed LED<br>TCP/IP Link LED<br>TCP/IP Duplex LED |
| **Real-time Clock Battery** | CR1225 3 V Lithium Battery |

| Communication Characteristics | |
|---|---|
| **RS-485** | Full-duplex data communication |
| **USB** | One USB host |
| **Ethernet** | One RJ-45 Ethernet connector |
| **Tamper** | Two inputs |

## 2.2 EXP-2024 Dual Reader Door Unit

| Electrical Characteristics | |
|---|---|
| **Operating Voltage** | 12–16VDC @ 1.0A |
| **Maximum Input Current** | Standby: 150 mA @ 12V<br>Maximum: 1000 mA @ 12V |
| **General Inputs** | 4 supervised high impedance inputs and 1 tamper input<br>Maximum voltage: 5 VDC |
| **Relay Outputs** | 4 relay outputs<br>5 A relay (N.O. or N.C.) |
| **Reader Ports** | 2 reader ports<br>Output voltage: 12 VDC<br>Max. output current: 300 mA<br>LED control output D0/D1, tamper input |

| Communication Characteristics | |
|---|---|
| **Tamper switches** | Front and back |
| **Visual Indicators** | Power LED |
| **Audio** | Sounder output (with BL-D40) |
| **Communication** | RS-485 |
| **Baud Rate** | 115200 bps |
| **Unit configuration** | 8 DIP switches<br>RS-485 serial address (1–32)<br>Tamper options |

## 2.3 EXP-2016 16-Relay Elevator Control Unit

| Electrical Characteristics | |
|---|---|
| **Operating Voltage** | 12–16 VDC @ 1.0 A |
| **Maximum Input Current** | Standby: 100 mA @ 12 V<br>Maximum: 800 mA @ 12 V |
| **General Inputs** | 1 tamper input<br>Maximum voltage: 5 VDC |
| **Relay Outputs** | 16-relay outputs<br>5 A Relay (N.O. or N.C.) |

| Communication Characteristics | |
|---|---|
| **Tamper switches** | Front and back |
| **Visual Indicators** | Power LED |
| **Communication** | RS-485 |
| **Baud Rate** | 115200 bps |
| **Unit configuration** | 8 DIP switches<br>RS-485 serial address (1–32)<br>Tamper options |

## 2.4 EXP-2088 8-Input/Output Interface

| Electrical Characteristics | |
|---|---|
| **Operating Voltage** | 12–16VDC @ 0.5A |
| **Maximum Input Current** | Standby: 100 mA @ 12 V<br>Maximum: 500 mA @ 12 V |
| **General Inputs** | 8 supervised high impedance inputs and1 tamper input<br>Maximum voltage: 5VDC |
| **Relay Outputs** | 8 relay outputs<br>5 A Relay (N.O. or N.C.) |

| Communication Characteristics | |
|---|---|
| **Tamper switches** | Front and back |
| **Visual Indicators** | Power LED |
| **Communication** | RS-485 |
| **Baud Rate** | 115200 bps |
| **Unit configuration** | 8 DIP switches<br>RS-485 serial address (1–32)<br>Tamper options |

## 2.5 EXP-3002 2-Channel Video Board

| Basic Characteristics | |
|---|---|
| **Input Power** | Input Vin 15 VDC<br>and battery of 12 VDC |
| **Input Current** | Standby: 450 mA at 15 VDC<br>Maximum: 1.5 A at 15 VDC |

| Integrated IP Characteristics | |
|---|---|
| **Web Server (Emb. Linux)** | Supports Browsers, FTP and TCP/IP Protocols |
| **Web Addressing** | DNS and IP Configuration,<br>MAC Address |
| **Bandwidth Management** | Selectivity of Traffic and Video Features:<br>Image size, compression, and fps |
| **Data management** | Backup, FLASH Firmware,<br>History Event Log and Audit Trail |

| | |
|---|---|
| **IP Streaming Client** | Customized Low Latency Streaming Client |
| **Security** | Multiple Authentication levels for users – Basic Encryption |

| **Video Server Characteristics** | |
|---|---|
| **Internal A/D MPEG-4 Video Encoder** | 2 analog video inputs supporting PAL and NTSC formats.<br>Resolution of up to D1 25 fps when using one camera or up to 8 fps with two cameras connected.<br>Two analog composite<br>(BNC x 2) – AGC (120 m) |
| **PTZ Support** | No |
| **Text Overlay** | Time, Date, and two Custom fields |
| **Video Compression** | MPEG-4 – SP/ASP – (ISO 14496-2) |
| **Audio Codec** | AGC Audio – Industry Standard – Mono with EQ and speech Codec |
| **Frame Rate** | One channel: 30 (NTSC) 25 (PAL) @ up to D1 resolution (Single Video)<br>Two channel: 8 fps @ up to D1 resolution (Dual Video) |
| **Communication** | TCP/IP |
| **Data Storage** | On-Board pre-alarm, post event timers, and custom recording preferences. On-board USB 2.0 connection for adding a USB 2.0 compliant flash drive for local DVR recording. |
| **Max Flash Drive Capacity** | 8 gigabytes |

| **Environmental Characteristics** | |
|---|---|
| **Operating Temp. Range** | 32°F to 120.2°F (0°C to 49°C) |
| **Operating Humidity** | 0 to 90% (non-condensing) |

## 2.6 System Environmental Characteristics

- **Operating Temp. Range:** 32°F to 120°F (0°C to 49°C)
- **Operating Humidity:** 0 to 90% (non-condensing)

# 3. ExpansE Architecture

This chapter comes to explain the difference between the various access control topologies with an emphasis on the benefits of the ExpansE topology as well as detailed explanation on the various ExpansE components and enclosures

## 3.1 Central versus Distributed Topology

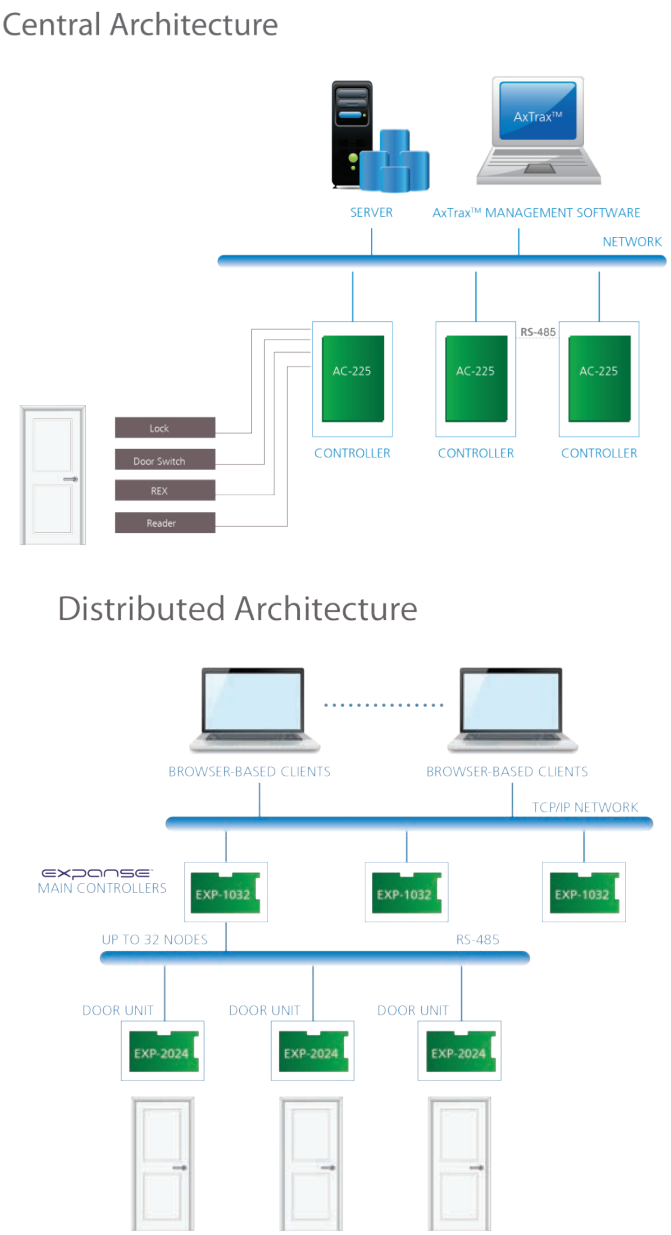
Central access control systems typically duplicate the hardware many times in order to cover large applications, and are often expensive, since they involve complicated and costly installation, configuration, networking, and cabling. Furthermore, since multiple controllers must be synchronized, it limits their performance and system capacity.

In a distributed system, the main networked controller unit (EXP-1032) is physically separated from the secondary units that manage the various door elements (such as readers, locks, REX buttons, switches and other I/Os) — substantially reducing cabling work and simplifying the installation process.

Distributed architecture allows systems to expand from a single door to thousands of doors in multiple sites, without unnecessary redundancy, and offers easy integration with external systems such as DVRs, Alarms, and more.

See Figure 1 for an explanatory comparison between Rosslare's AC-225 networked access control system as a central architecture and that of Rosslare's new ExpansE distributed architecture.

**Figure 1: Central versus Distributed Architectures**



## 3.2 ExpansE Distributed Access Control

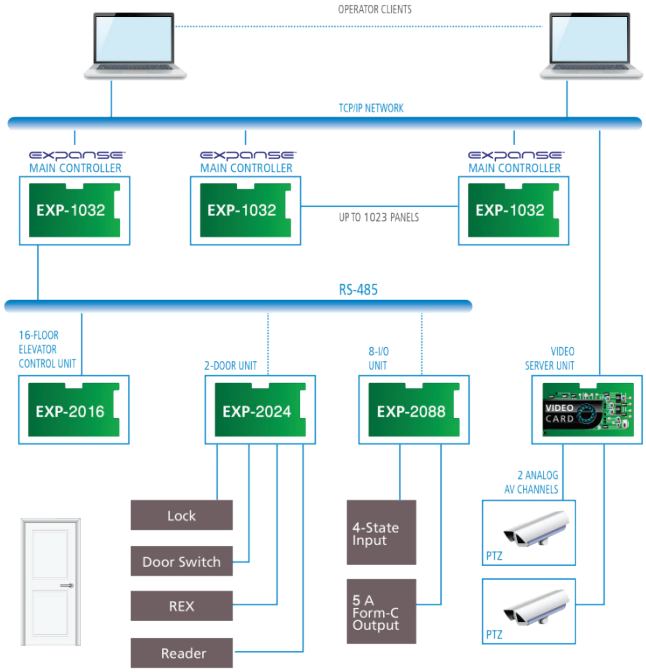
The ExpansE system supports up to 2,048 Networked controllers (MUs), one designated as the master and the rest as slaves connected over an Ethernet network, each of these MUs are then connected to various EUs via RS-485 connection.

The ExpansE system offers various EUs including dual reader door unit, an 8-I/O interface, dedicated 16-relay elevator control unit and many more.

Based on distributed architecture, each one of the ExpansE's EUs (for example, a door or I/O) is physically separated from the MU, which controls up to 32 EUs. Each of the MUs can manage up to 256 inputs, 512 outputs or 32 doors. The panels are controlled by a web based application embedded into the controller and also has an optional server based software.

The ExpansE system also offers several mounting options to best respond to each specific need, be it a small singular box for individual units, a specially designed box which includes an integrated power supply and backup battery, or a rack mount which can hold several MUs, EUs or a combination of both. Figure 2 shows an example setup for a distributed network of the ExpansE access control system.

**Figure 2: Sample of ExpansE Configuration**



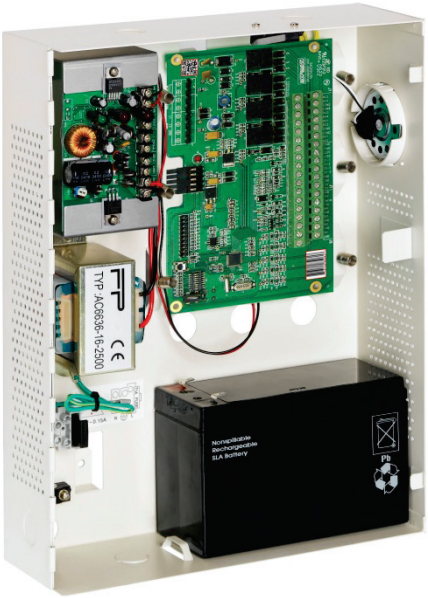
## 3.3 ExpansE Mounting Options

The ExpansE units come in various mounting options be it as a MU or EU board, or a board mounted in one of several box types as described below.

### 3.3.1 ME-01 Single Board Self-Powered Metal Enclosure

This sturdy, lockable, metal case has room for a single board along with a power supply and backup battery, see Figure 3.

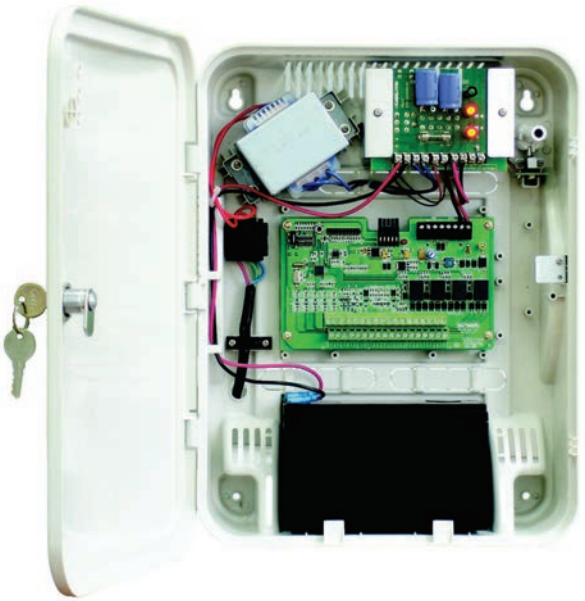
**Figure 3: ME-01 Single-Board Self-Powered Metal Enclosure**




### 3.3.2 ME-12 Single Board Self-Powered Plastic Enclosure

The ME-12 plastic enclosure holds a single board along with a power supply and backup battery. The wiring ducts and holders secure both the various components and the wiring within the enclosure. The enclosure's lockable door is designed to be easily removed when opened for better access during installation, yet cannot be removed when the door is closed in normal use (see Figure 4).

**Figure 4: ME-12 Single-Board Self-Powered Plastic Enclosure**



### 3.3.3 ME-14 Compact Single Board Self-Powered Enclosure

The ME-14 is a simple plastic enclosure suited for a singular board (see Figure 5).

**Figure 5: ME-14 Compact Single-Board Self-Powered Enclosure**

### 3.3.4 ME-00 9-Board Tray Cabinet Housing

The ME-00 offers a rack which can hold several MUs, EUs or a combination of both. The rack holds one 14 Ah backup battery as well as a power supply which powers all the connected units (see Figure 6).

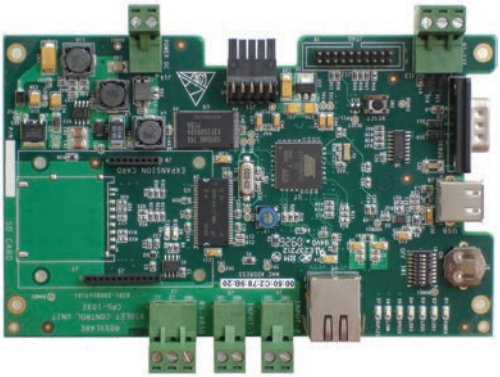
**Figure 6: ME-00 9-Board Tray Cabinet Housing**

## 3.4 ExpansE Hardware Units

The ExpansE system is comprised of several hardware units, the MU, EXP-1032 ExpansE Networked Controller, and several EUs such as the EXP-2024 Dual Reader Door Unit, EXP-2016 16-Relay Elevator Control Unit, and the EXP-2088 – 8-Input/Output Interface.

### 3.4.1 EXP-1032 ExpansE Networked Controller

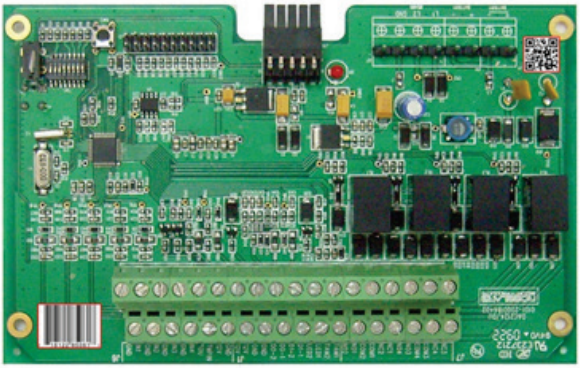
**Figure 7: EXP-1032 ExpansE Networked Controller**



- Supports 32 EUs, which can include up to 32 doors/64 readers, up to 256 inputs and 512 outputs, as well as up to 128,000 users per controller
- 100,000 history event log size
- On-board Ethernet, RS-485 and USB (host) 2.0 ports

### 3.4.2 EXP-2024 Dual Reader Door Unit

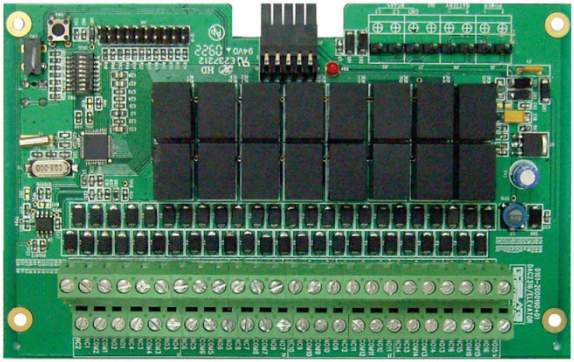
**Figure 8: EXP-2024 Dual Reader Door Unit**



- Two reader ports – supports Wiegand 26 bits and other standard and non-standard formats
- Four four-state inputs, 4 form-C relay outputs, and a sounder output
- RS-485 communication ports

### 3.4.3 EXP-2016 16-Relay Elevator Control Unit

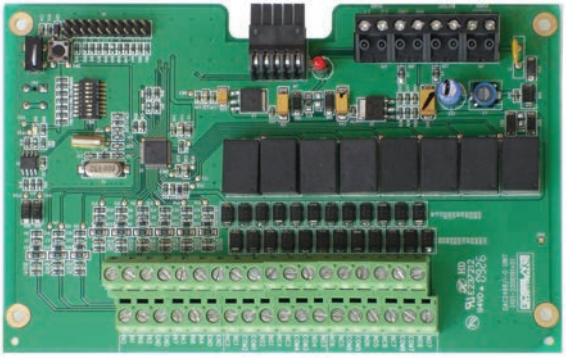
**Figure 9: EXP-2016 16-Relay Elevator Control Unit**



- 16 Form-C relay outputs, ideal for elevator control applications
- RS-485 communication ports

### 3.4.4 EXP-2088 8-Input/Output Interface Unit

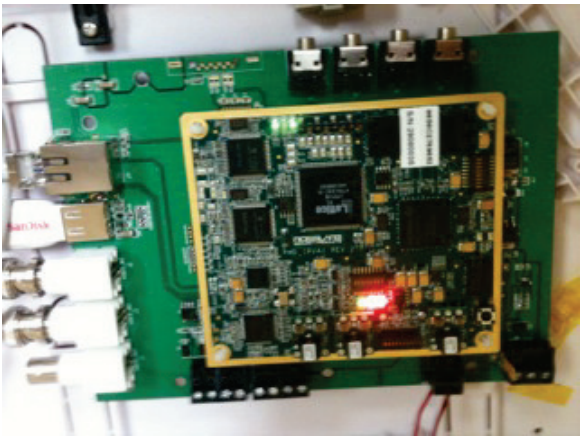
**Figure 10: EXP-2088 8-Input/Output Interface Unit**



- Eight four-state inputs and 8 form-C relay outputs
- RS-485 communication ports

### 3.4.5 EXP-3002 2-Channel Video Board

**Figure 11: EXP-3002 2-Channel Video Board**



## 3.5 Reports Production and Backup Software

The ExpansE system is complemented with the ExClouds software (see Chapter 10).

## 3.6 Card Readers and Keypads

Each Door Unit can be connected to a maximum of two readers. There are four types of readers supported:

- Biometric Readers
- Card readers
- Keypads
- Dual keypad & card readers

A keypad is required for any reader mode that requires PIN code entries, such as "Card or PIN", "PIN Only" or "Card and PIN (Secured mode)".

# 4. Hardware Installation

Each MU needs to be wired and defined in the web based application along with its associated EUs separately.

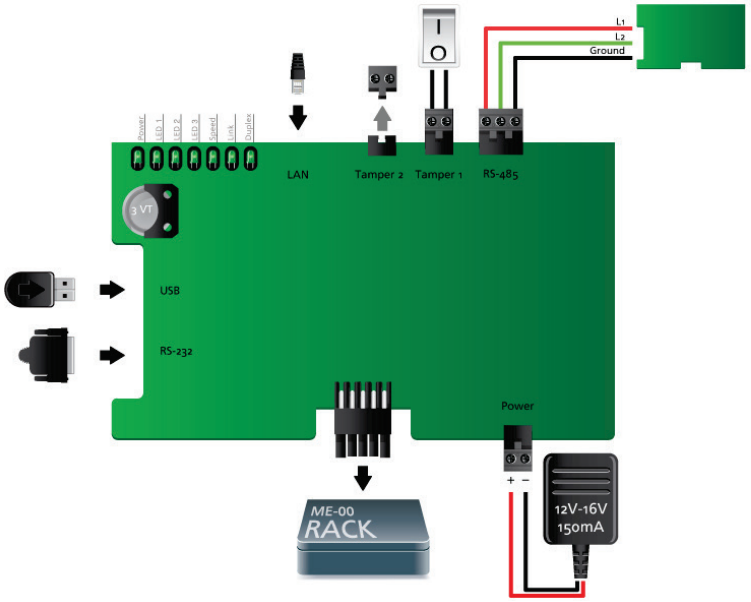
## 4.1 Wiring Instructions

The wiring chapter is divided per units showing the various connections unique to each board, followed by general instructions applicable to several units.

### 4.1.1 EXP-1032 ExpansE Networked Controller

The EXP-1032 MU board and its components as well as general connections from the MU are shown in Figure 12.

**Figure 12: EXP-1032 ExpansE Networked Controller Wiring**




*To wire the EXP-1032 ExpansE networked controller:*

1. Connect a 12–16 VDC 1500 mA transformer to the power terminal block (see Section 4.3).
2. Connect the EUs to the MU using daisy chain methodology, using the RS-485 terminal block. See Section 4.4 for detailed instructions.
3. When placing the MU into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

Note

When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect a tamper switch to the tamper input terminal block. See Section 4.5.2.3.
5. Connect the RJ-45 cable to the LAN socket in the wall and the other end to the LAN socket on the MU board.

### 4.1.2 EXP-2024 Dual Reader Door Unit

The EXP-2024 unit and its components are shown in Figure 13. Detailed wiring instructions are explained below and shown in Figure 14.

When connecting a reader, the following should be defined:

| | |
|---|---|
| **Single door controller:** | Door 1 – Reader 1 IN<br>Door 1 – Reader 2 OUT |
| **Double door controller:** | Door 1 – Reader 1 IN<br>Door 2 – Reader 2 IN |

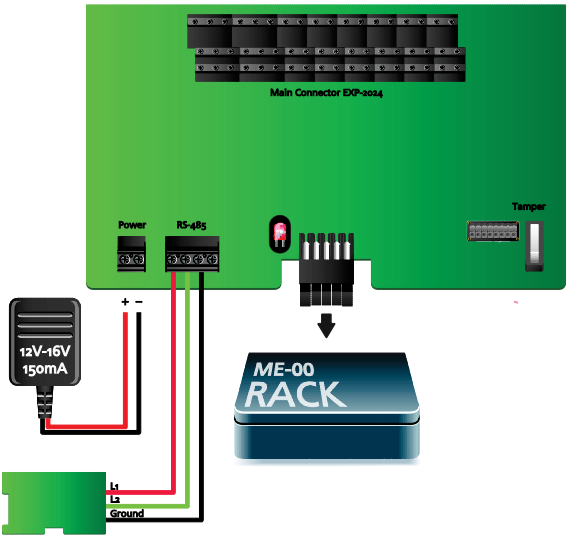
Use the ExpansE web application to set the readers for single or dual door operation as well as IN or OUT usage. Additionally set the data transmission format for each reader. See Sections 7.2 and 7.4.

The reader's tamper output connects to the access control panel's Reader-Tamper input. If the reader is interfered with, an alarm can be generated.

The panel's Reader G.LED output activates the reader's green LED input when operating in "Card and PIN" secure mode. While this mode is activated, users must enter a PIN on the keypad immediately after presenting the card.

The controller activates the LED control for 2 seconds when an access granted event occurs.

**Figure 13: EXP-2024 Dual Reader Door Wiring**




*To wire the EXP-2024 Dual Reader Door Unit:*

1. Connect a 12-16VDC 1500 mA transformer to the power terminal block (see Section 4.3).
2. Connect the RS-485 communication terminal block to the controller using daisy chain methodology. See Section 4.4 for detailed instructions.
3. When placing the EXP-2024 into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

> Note
>
> When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect the reader(s) to the EXP-2024 using Table 1 as a reference.

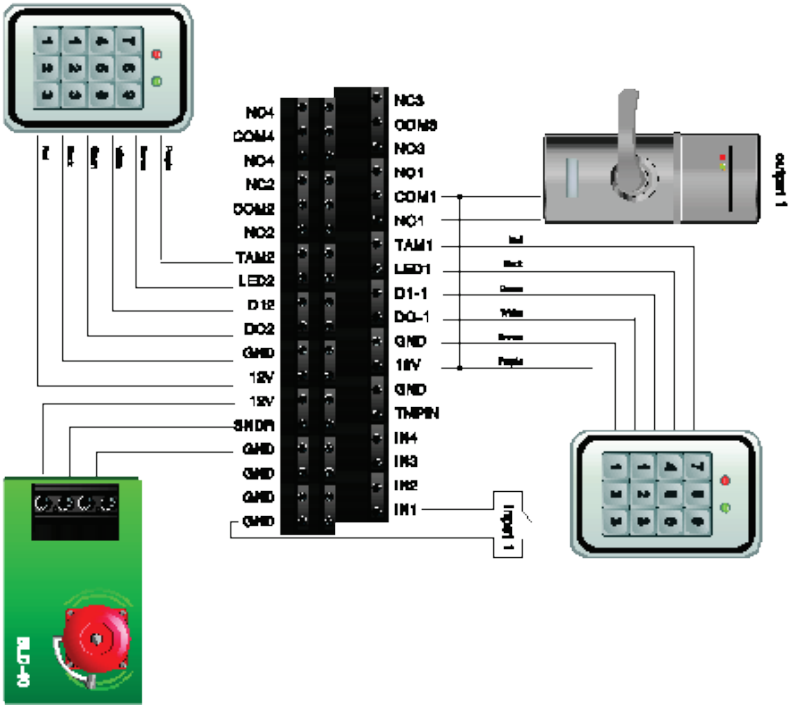
   If the tamper output is being utilized, connect the purple wire to the tamper input on the EXP-2024.

**Table 1: EXP- 2024 Dual Reader Door Unit Wiring Details**

| Color | Wiegand Output |
|---|---|
| Red | +DC Input |
| Black | Ground |
| White | Data 1 / Clock |
| Green | Data 0 / Data |
| Brown | LED/Buzzer Control |
| Purple | Tamper |

5. Connect a tamper switch to the tamper input terminal block (see Section 4.5.2.3). There are 4 inputs on the EXP-2024 (see Section 4.5 for detailed wiring instructions and uses).
6. There are 4 outputs on the EXP-2024 board that can be used for various applications (see Section 4.5.3 for detailed wiring instructions and uses).
7. You have the option of connecting Rosslare's BLD-40 sounder see the BLD-40 manual for wiring instructions.

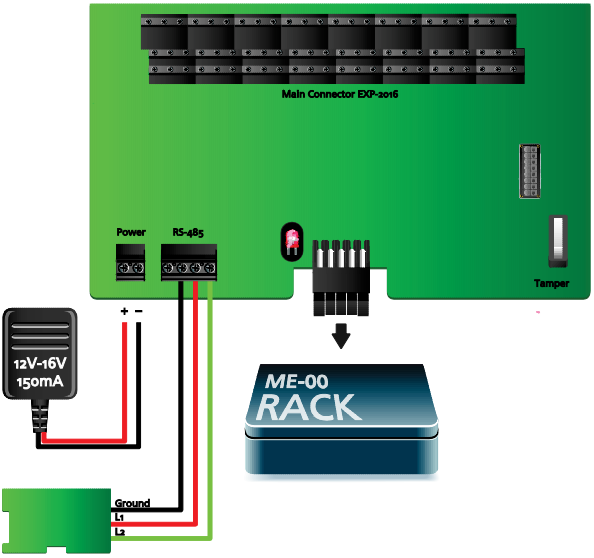
**Figure 14: EXP- 2024 Dual Reader Door Unit Wiring Details**



### 4.1.3 EXP-2016 16-Relay Elevator Control Unit

The EXP-2016 board and its components are shown in Figure 15; detailed wiring instructions are explained below and shown in Figure 16.

**Figure 15: EXP-2016 16-Relay Elevator Control Unit Wiring**



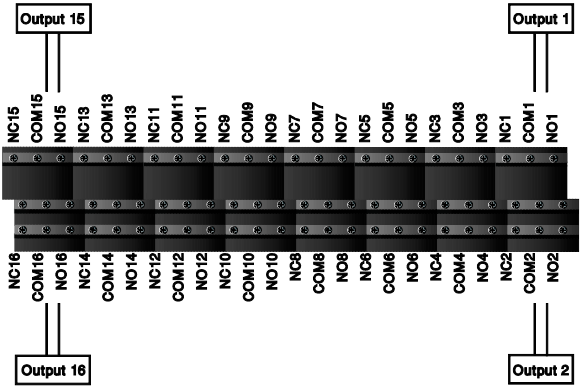

*To wire the EXP-2016 16-Relay Elevator Control Unit:*

1. Connect a 12-16VDC 1500 mA transformer to the power terminal block (see Section 4.3).
2. Connect the RS-485 communication terminal block to the EXP-2016 using daisy chain methodology. See Section 4.4 for detailed instructions.
3. When placing the EXP-2016 into the ME-00 rack mount, remove the Power terminal block and slide the controller into the slot, making sure the ME-00 Molex connector is secured.

> **Note**
> When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. There are 16 outputs on the EXP-2016 board that can be used for various applications. See Section 4.5.3 for detailed wiring instructions and uses. See Appendix A for an example of how to wire an elevator unit.

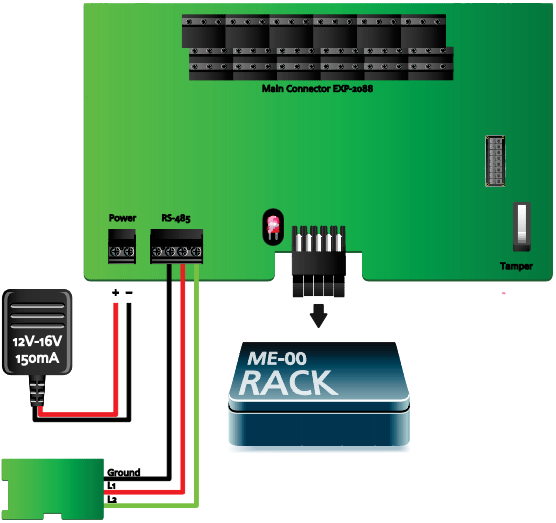
**Figure 16: EXP-2016 16-Relay Outputs Elevator Control Unit Wiring**


Output 15
Output 1
NC15 COM15 NO15 NC13 COM13 NO13 NC11 COM11 NO11 NC9 COM9 NO9 NC7 COM7 NO7 NC5 COM5 NO5 NC3 COM3 NO3 NC1 COM1 NO1
NC16 COM16 NO16 NC14 COM14 NO14 NC12 COM12 NO12 NC10 COM10 NO10 NC8 COM8 NO8 NC6 COM6 NO6 NC4 COM4 NO4 NC2 COM2 NO2
Output 16
Output 2

### 4.1.4 EXP-2088 – 8-Input/Output Interface

The EXP-2088 and its components are shown in Figure 17 detailed wiring instructions are explained below and shown in Figure 18.

**Figure 17: EXP-2088 8-Input/Output Interface Wiring**




*To wire the EXP-2088 8-Input/Output Interface Unit:*

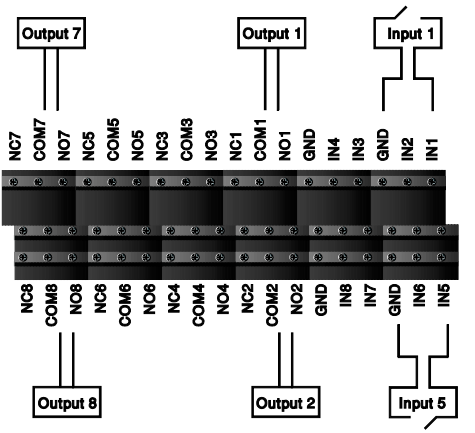
1. Connect a 12-16VDC 1500mA transformer to the power terminal block (see Section 4.3).
2. Connect the RS-485 communication terminal block to the EXP-2088 board using daisy chain methodology. See Section 4.4 for detailed instructions.

3. When placing the EXP-2088 into the ME-00 rack mount, remove the Power terminal block and slide the EXP-2088 into the slot, making sure the ME-00 Molex connector is secured.

When using the ME-00 rack mount, the power and RS-485 communication connection are received from the rack itself and do not require direct wiring.

4. Connect a tamper switch to the tamper input terminal block (see Section 4.5.2.3). There are 8 inputs on the EXP-2088 board, see Section 4.5 for detailed wiring instructions and uses.
5. There are 8 outputs on the EXP-2088 board that can be used for various applications, see Section 4.5.3 for detailed wiring instructions and uses.

**Figure 18: EXP-2088 8-Input/Output Interface Detailed Wiring**

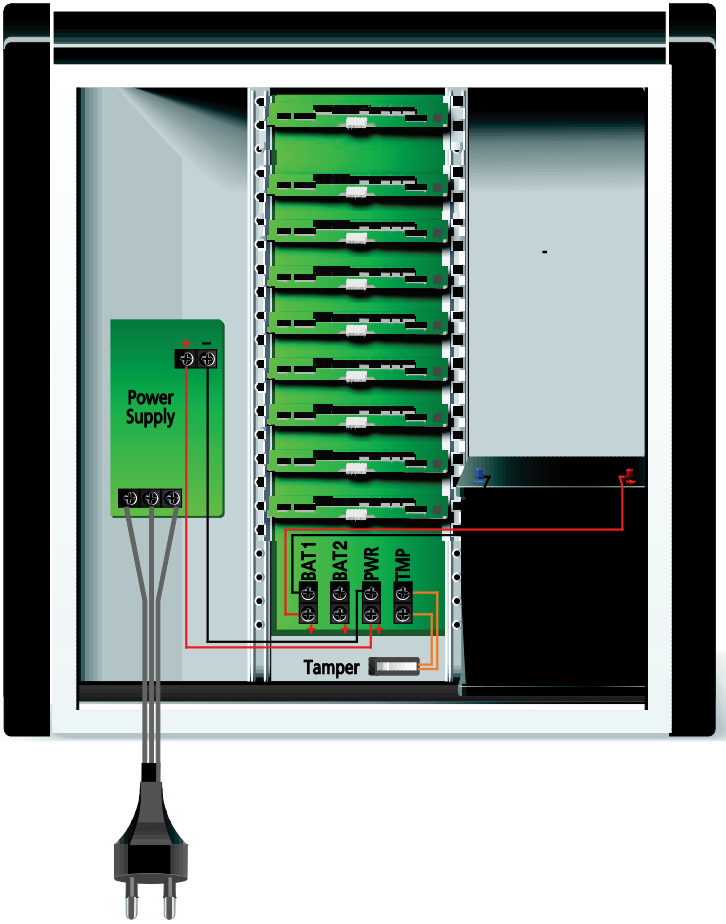



## 4.2 ME-00 9-Board Tray Cabinet Housing Wiring

The ME-00 9-Board Tray Cabinet Housing can be used to store several MUs and/or EUs. The Cabinet provides internal RS-485 communication between the units as well as power to each of the connected units.

See the detailed wiring instructions below on wiring the cabinet itself as well as Figure 19.

**Figure 19: ME-00 9-Board Tray Cabinet Housing Wiring**




*To wire the ME-00 9-Board Tray Cabinet Housing:*

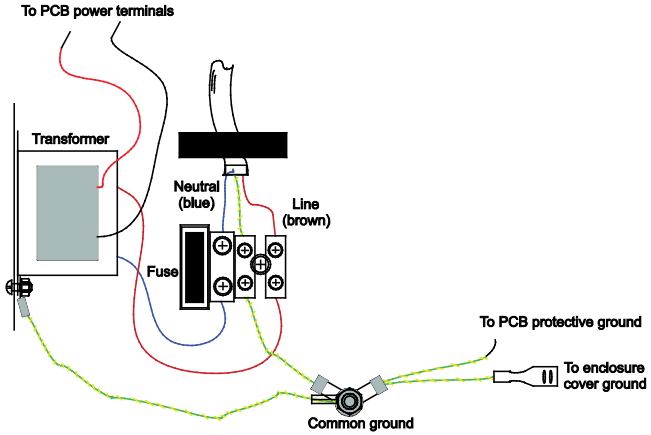
1. Connect a 12-16 VDC 1500 mA transformer to the power terminal block (see Section 4.3).
2. Connect the backup battery to the battery terminal block.
3. Connect a tamper switch to the tamper input terminal block (see Section 4.5.2.3).

## 4.3 Power Supply

The following diagram illustrates the wiring between the DC adaptor and the ExpansE units, as well as the cabinet Power supply connection. It is recommended to add a 12VDC lead acid backup battery if the main power

supply fails. Backup battery must be used if implementing the connection of lock devices to the units, when more than 1A of current is required.

**Figure 20: Wiring the Power Supply**




## 4.4 RS-485 Daisy Chain

A daisy chain connection allows the connection of up to 32 EUs to the MU along a single serial line.

The MU is connected directly to the LAN network and the associated EUs are connected to the MU.

Note

It is important to connect the Ground between all the connected units. The purpose of this connection is to have a single reference line.

At each end of the data line, a termination resistor of 120Ω may be required. Apply the resistor across the L1 and L2 connections. These termination resistors are especially important in long cable runs.

Note

Other connections can optionally be used in addition to L1 and L2 for communication reference.

## 4.5 Inputs and Outputs

The input and output connections detailed in this chapter are applicable to all inputs and outputs of the ExpansE system.

### 4.5.1 Input Types

Each input can be set as one of six input types – Normally Open, Normally Closed, Normally Open Supervised with 1 or 2 resistors, and Normally Closed Supervised with 1 or 2 resistors.

Inputs IN1, IN1A, IN2, and IN2A may be configured individually as either supervised or non-supervised inputs.

Non-supervised inputs have two states:

- Normal State – N.C. or N.O.
- Opposite State – N.O. or N.C.

Supervised inputs have three states:

- Normal State
- Abnormal State
- Trouble State

The Trouble state is caused by either tampering with the input circuit or by faulty hardware installation. Once configured as supervised input, add a resistor of 2.2 KΩ, 8.2 KΩ, or both on the input circuit. See the following diagrams.

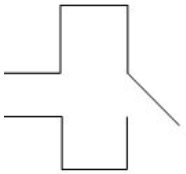
#### 4.5.1.1 Normally Open Input Connection

Normally Open Input has 2 states:

- Switch Open – Normal State:
  Loop resistance = Infinite (open circuit).
- Switch Closed – Abnormal State:
  Loop resistance = 0 (short circuit).

**Figure 21: Normally Open Input Connection**

Normally Open Switch (N.O.)

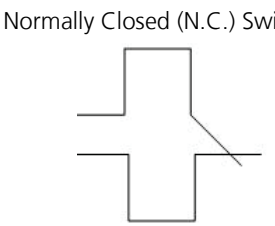


#### 4.5.1.2 Normally Closed Input Connection

Normally Closed Input has two states:

- Switch Closed – Normal State:
  Loop resistance = 0 (short circuit)
- Switch Open – Abnormal State:
  Loop resistance = Infinite (open circuit)

**Figure 22: Normally Closed Input Connection**



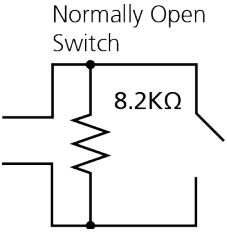

4.5.1.3 Normally Open Supervised Single Resistor Input Connection

Connect an 8.2KΩ resistor in parallel to the input switch contacts.

Normally Open Supervised Input has 3 states:

- Switch Open – Normal State:
  Loop resistance = 8.2KΩ
- Switch Closed – Abnormal State:
  Loop resistance = 0 (short circuit)
- Open circuit across input terminals – Trouble State:
  Loop resistance = Infinite (open circuit)

**Figure 23: Normally Open Supervised Input (Single Resistor)**




4.5.1.4 Normally Open Supervised Double Resistor Input Connection

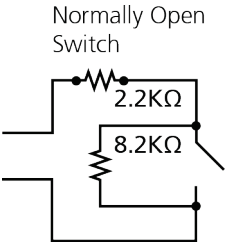
Connect a 2.2KΩ resistor in series to the input switch contacts.

Connect an 8.2KΩ resistor in parallel to the input switch contacts.

Normally Open Supervised Input has 3 states:

- Switch Open – Normal State:
  Loop resistance = 10.4 KΩ
- Switch Closed – Abnormal State:
  Loop resistance = 2.2 KΩ
- Open circuit (Infinite loop resistance) or short circuit (0 resistance) across input terminals – Trouble State

**Figure 24: Normally Open Supervised Input (Double Resistor)**



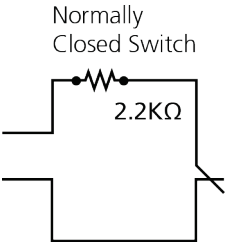

4.5.1.5 Normally Closed Supervised Single Resistor Input Connection

Connect a 2.2KΩ resistor in series to the input switch contacts.

Normally Closed Supervised Input has 3 states:

- Switch Closed – Normal State:
  Loop resistance = 2.2 KΩ
- Switch Open – Abnormal State:
  Loop resistance = Infinite (open circuit)
- Short circuit across input terminals – Trouble State:
  Loop resistance = 0 (short circuit)

**Figure 25: Normally Closed Supervised Input (Single Resistor)**




4.5.1.6 Normally Closed Supervised Double Resistor Input Connection

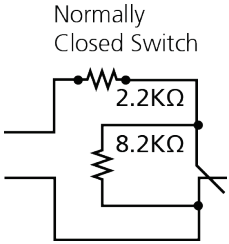
Connect a 2.2 KΩ resistor in series to the input switch contacts.

Connect an 8.2 KΩ resistor in parallel to the input switch contacts.

Normally Closed Supervised Input has 3 states:

- Switch Closed – Normal State:
  Loop resistance = 2.2KΩ
- Switch Open – Abnormal State:
  Loop resistance = 10.4KΩ
- Open circuit (Infinite loop resistance) or short circuit (0 resistance) across input terminals – Trouble State

**Figure 26: Normally Closed Supervised Input (Double Resistor)**




### 4.5.2 Inputs Description

This chapter describes the inputs default operation.

#### 4.5.2.1 Request to Exit Button (REX) Input

Use the REX Input to open a door directly. Typically, the REX input is connected to a Normally Open push button that is located inside the premises. The push button is generally located in an easy-to-access position and opens a door without reading a proximity card or PIN code.

| | |
|---|---|
| **Single door controller:** | Door 1 – IN 1 |
| **Double door controller:** | Door 1 – IN 1<br>Door 2 – IN 2 |

#### 4.5.2.2 Door Monitor Input

The Door Monitor Input typically connects to a Normally Closed door sensing micro-switch for door status monitoring. Using Door Monitor enables many advanced options such as door forced alarm warning, door held open warning, interlocking doors and more. The following should be defined:

| | |
|---|---|
| **Single door controller:** | Door 1 – IN 1A<br>Door 1 – IN 1.A |
| **Double door controller:** | Door 2 – IN 2A |

#### 4.5.2.3 General Purpose Inputs

These are free inputs that can be used for various functions. The following should be defined:

| | |
|---|---|
| **Single door controller:** | Door 1 – IN 2<br>Door 1 – IN 2A |
| **Double door controller:** | No general purpose input available |

General purpose inputs are suitable for most uses. For example, they might be used to detect tampering, to activate alarm sensors or for monitoring power supply failure.

### 4.5.3 Output Description

This chapter describes the inputs default operation.

Rosslare Security recommends the use of suppression diodes for all outputs that activate an inductive load.

#### 4.5.3.1 Door Lock – Power Enabled Output

There are two types of door locking devices:

- Fail open (fail secure)
- Fail close (fail safe)

The following should be defined:

| | |
|---|---|
| **Single door controller:** | Door 1 – OUT 1 |
| **Double door controller:** | Door 1 – OUT 1<br>Door 2 – OUT 2 |

An ExpansE output can provide 12VDC power up to 1A for external door locks. For higher rated door locks an external UL 294 Listed power supply must be used to provide power to the door lock.

For UL installations, the installer must configure the system as fail-safe to comply with NFPA (National Fire Protection Association) regulations.

#### 4.5.3.2 Elevator – Non-power Output

When using the elevator control output to close the elevator key relay switch, there is no need to supply power to the circuit. There is an option to choose between Normally Open or Normally Closed circuits.

The circuit is based on wiring the common output together with either the N.O. or N.C. output to the elevator key switch thus closing the electric circuit.

## 4.6 Output Wiring

Figure 27 and Figure 28 illustrate wiring for two main types of 12VDC electrical release mechanisms. Other electrical devices can be switched using the voltage free relay contacts.

Figure 27: Power Enabled Output Wiring

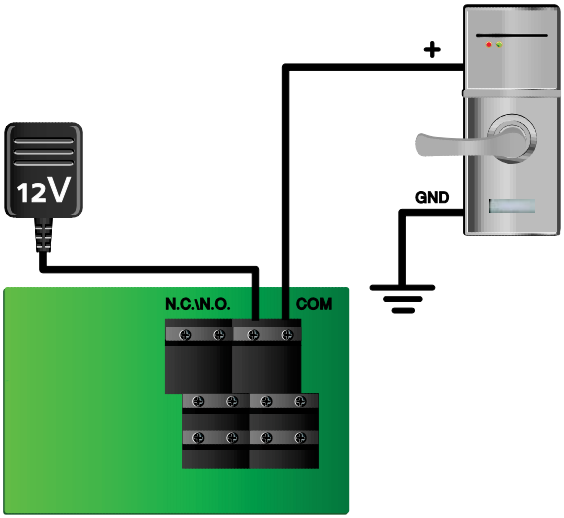
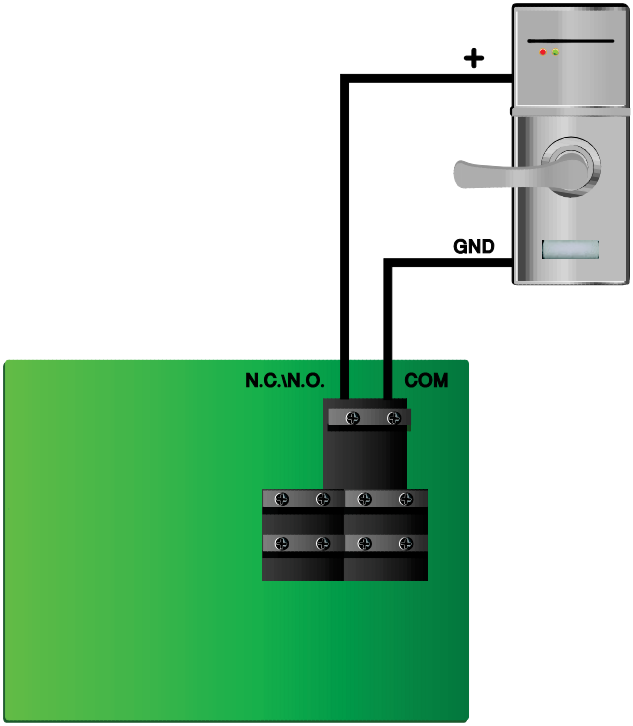



Figure 28: Non-Power Output Wiring



## 4.7 Mounting

This chapter shows how to mount and assemble each of the available boxes of the ExpansE system.

### 4.7.1 ME-01 Single Board Self-Powered Metal Enclosure

The ME-01 is a sturdy, lockable, metal case that has room for a single MU or EU board along with a power supply and backup battery.

*To install the ME-01:*

1. Using the holes dimensions and locations shown in Figure 29, drill holes in the wall.
2. Insert masonry anchors into the drilled holes.
3. Wire the unit according to the wiring instructions as explained in Section 4.1.
4. Mount the ME-01 enclosure onto the wall as shown in Figure 30.
5. Mount the MU or EU board in the enclosure using the spacers supplied and connect the in-box power and backup battery as shown in Figure 31.
6. Close and secure the enclosure.

**Figure 29: ME-01 Mounting Template**

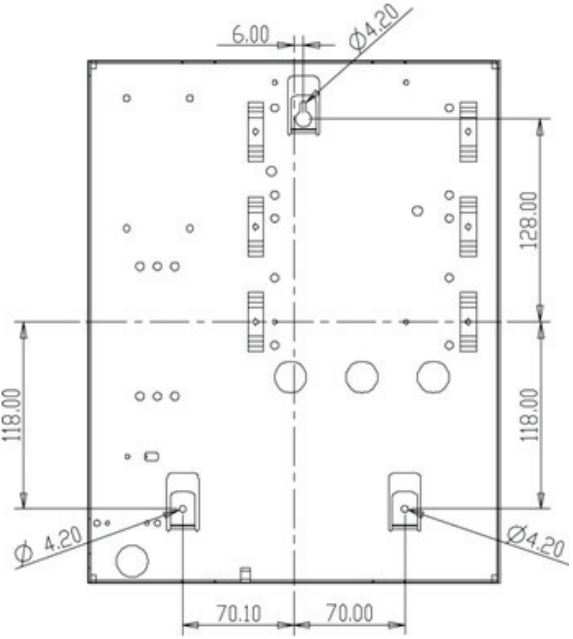


**Figure 30: ME-01 Wall Mounting**

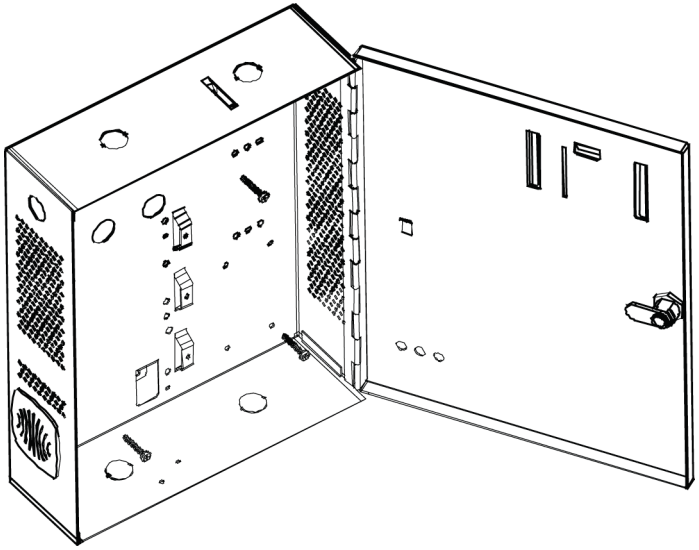
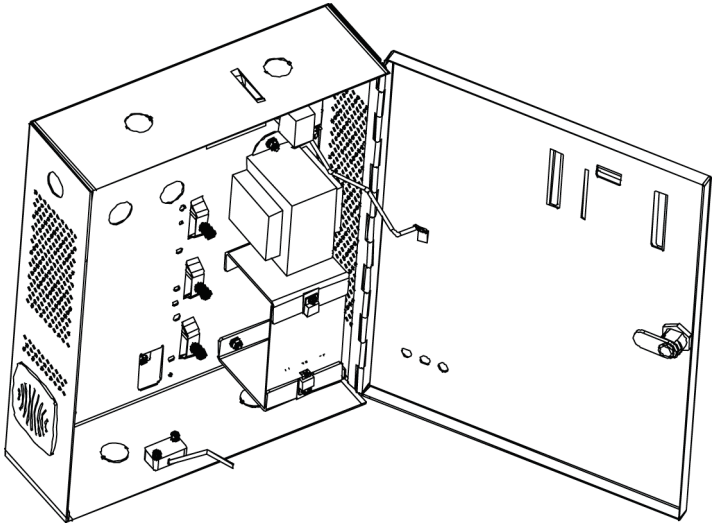


**Figure 31: ME-01 Unit Mounting and In-Box Connections**



### 4.7.2 ME-12 Single Board Self-Powered Plastic Enclosure

The ME-12 specially designed plastic enclosure holds a single MU or EU board along with a power supply and backup battery.

*To install the ME-12:*

1. Using the holes dimensions and locations shown in Figure 32, drill holes in the wall.
2. Insert masonry anchors into the drilled holes.
3. Wire the unit according to the wiring instructions as explained in Section 4.1.
4. Mount the ME-12 onto the wall as shown in Figure 33.
5. Mount the MU or EU board in the enclosure using the spacers supplied and connect the in-box power and backup battery as shown in Figure 34, make sure to run the wires through the specifically designed wiring ducts.
6. Secure the backup battery and other loose components using the specifically designed openings and slots.
7. Close and secure the enclosure door.

**Figure 32: ME-12 Mounting Template**

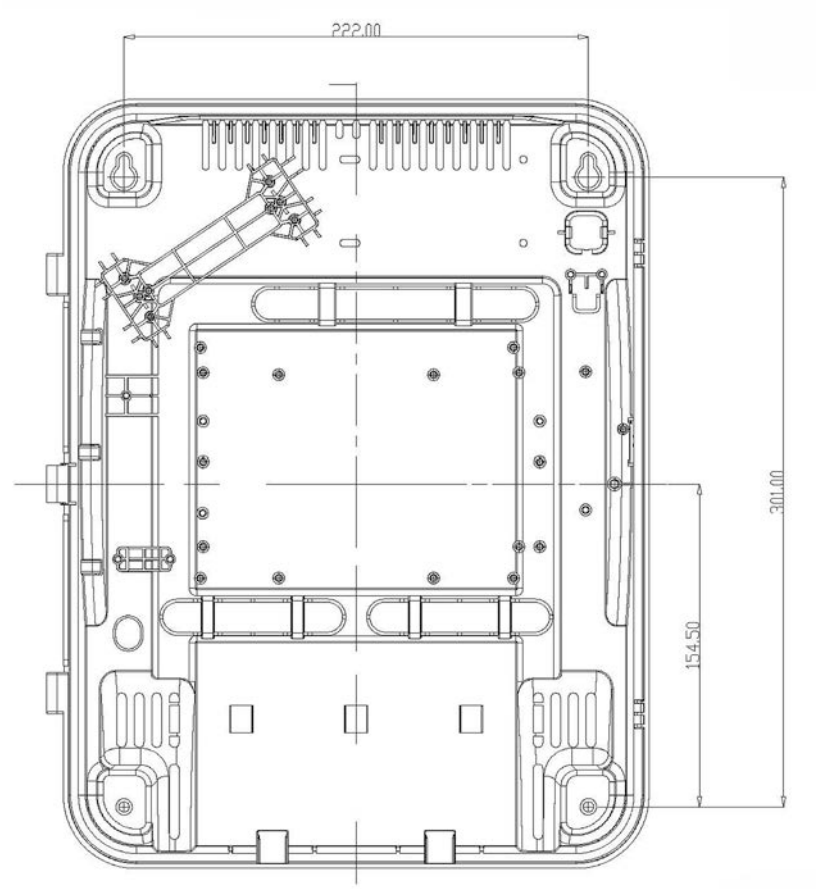


**Figure 33: ME-12 Wall Mounting**

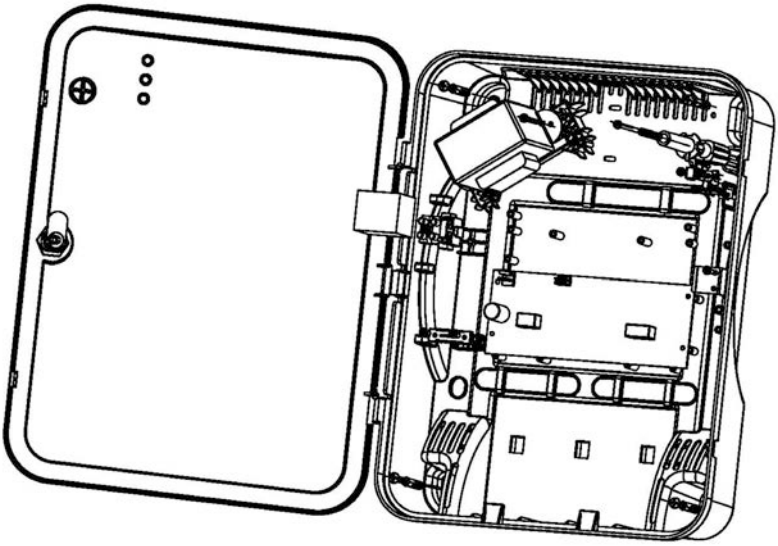
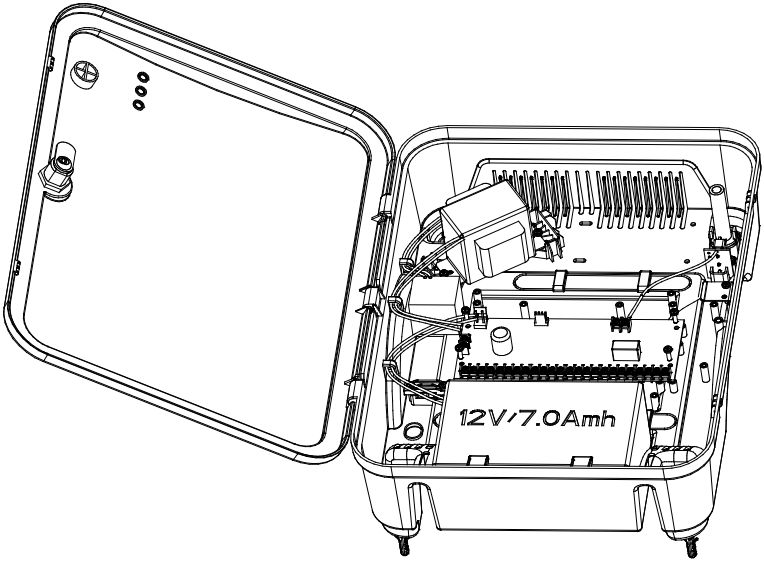


**Figure 34: ME-12 Unit Mounting, In-Box Connections and Wiring**



### 4.7.3 ME-14 Compact Single Board Self-Powered Enclosure

The ME-14 is a simple plastic casing suited for a singular MU or EU board.

*To install the ME-14:*

1. Open the ME-14 case using a screw driver.
2. Using the ME-14's back plate as a template drill holes in the wall (see also Figure 35 for dimension reference).
3. Insert masonry anchors into the drilled holes.
4. Wire the unit according to the wiring instructions as explained in Section 4.1.
5. Mount the ME-14 onto the wall.
6. Mount the MU or EU board in the case and reassemble the casing as shown in Figure 36.

Note

The ME-14 has no room for a backup battery charger.

It can be used without a backup battery or by drawing lines from the MU backup battery to the unit.

**Figure 35: ME-14 Mounting Template**

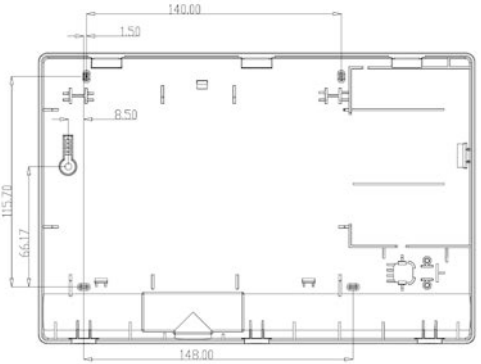
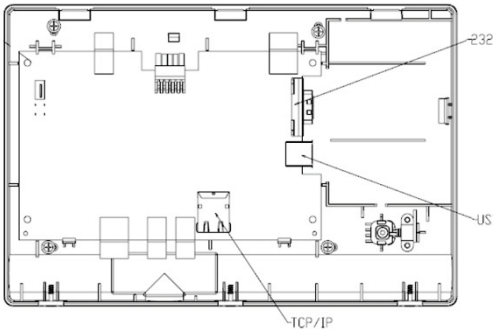



**Figure 36: ME-14 Assembly**



### 4.7.4 ME-00 9-Board Tray Cabinet Housing

The ME-00 9-Board Tray Cabinet Housing offers a cabinet that holds several MUs and/or EUs. The cabinet also holds several backup batteries as well as an embedded power supply, which powers all the connected units.

*To install the ME-00:*

1. Using the holes dimensions and locations shown in Figure 37 drill holes in the wall.
2. Insert masonry anchors into the drilled holes.
3. Wire the cabinet as described in Section 4.2.
4. Slide and secure the individual units into the designated slots, ensure that each unit is secured in place to receive the power and communication directly from the rack as shown in Figure 38.
5. Thread the wires through the designated holes in the rear of the rack as shown in Figure 39, wire the individual units according to the wiring instructions as explained in Section 4.1.
6. Mount the ME-00 onto the wall.
7. Close and secure the enclosure.

**Figure 37: ME-00 Mounting Template**

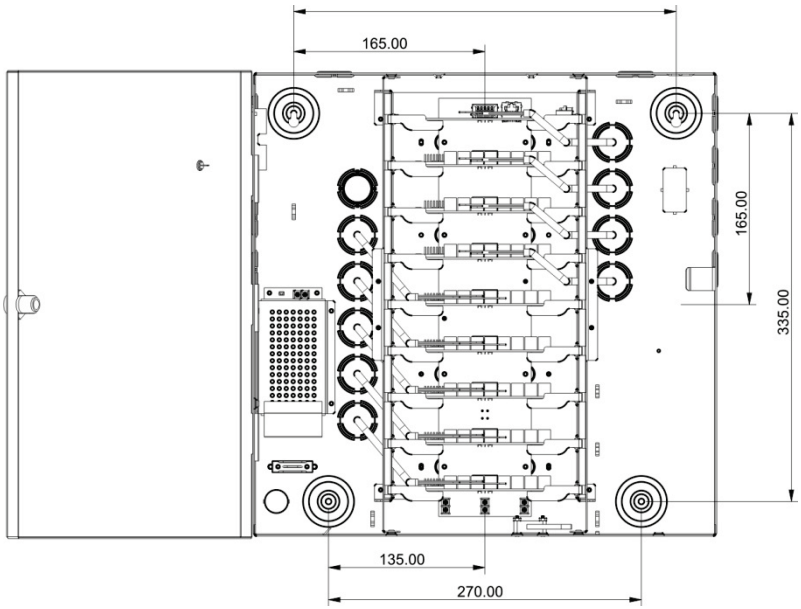


Figure 38: ME-00 Units Placement

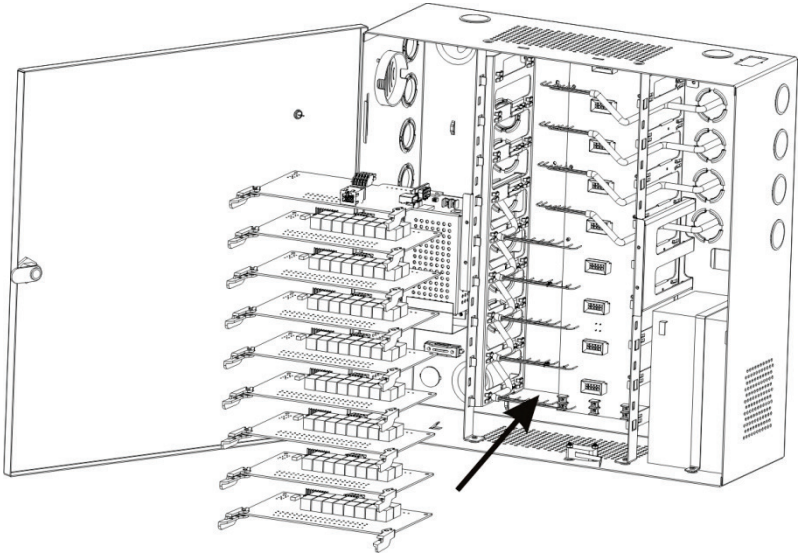
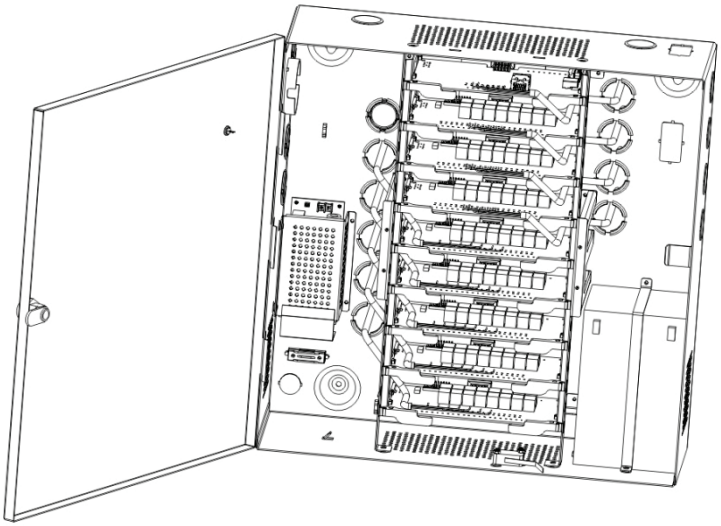


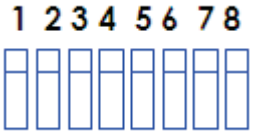
Figure 39: ME-00 Wiring Threads



## 4.8 DIP Switch Configuration

The ExpansE units have a DIP switch that controls a number of operating parameters including the device address and tamper settings.

**Figure 40: DIP Switches**




The following is a list of DIP switch numbers in the units and their functions:

| Switch # | Function |
|---|---|
| 1 | The ExpansE Units network address |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | Reserved for factory use, set to ON at all times |
| 7 | Front and Back Tamper switch Enabled/Disabled |
| 8 | |

Note

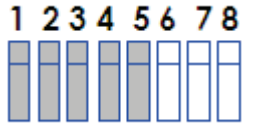
Power down the System before changing the DIP switches settings. After changes have been made, restart the system. The new settings are automatically defined after power up.

### 4.8.1 Network Addressing

The first 5 DIP switches are used to select the binary coded access control unit internal network address.

The default network address is set to "1".

**Figure 41: Internal Network Address DIP Switch Setting**




Note

For successful communications, the DIP switch must match the address set in the ExpansE web application.

Table 2 displays the 32 DIP switch settings available:

**Table 2: Available DIP Switch Settings**

| Address | Switch 1 | Switch 2 | Switch 3 | Switch 4 | Switch 5 |
|---|---|---|---|---|---|
| 1 | Off | Off | Off | Off | Off |
| 2 | Off | Off | Off | Off | On |
| 3 | Off | Off | Off | On | Off |
| 4 | Off | Off | Off | On | On |

| Address | Switch 1 | Switch 2 | Switch 3 | Switch 4 | Switch 5 |
|---|---|---|---|---|---|
| 5 | Off | Off | On | Off | Off |
| 6 | Off | Off | On | Off | On |
| 7 | Off | Off | On | On | Off |
| 8 | Off | Off | On | On | On |
| 9 | Off | On | Off | Off | Off |
| 10 | Off | On | Off | Off | On |
| 11 | Off | On | Off | On | Off |
| 12 | Off | On | Off | On | On |
| 13 | Off | On | On | Off | Off |
| 14 | Off | On | On | Off | On |
| 15 | Off | On | On | On | Off |
| 16 | Off | On | On | On | On |
| 17 | On | Off | Off | Off | Off |
| 18 | On | Off | Off | Off | On |
| 19 | On | Off | Off | On | Off |
| 20 | On | Off | Off | On | On |
| 21 | On | Off | On | Off | Off |
| 22 | On | Off | On | Off | On |
| 23 | On | Off | On | On | Off |
| 24 | On | Off | On | On | On |
| 25 | On | On | Off | Off | Off |
| 26 | On | On | Off | Off | On |
| 27 | On | On | Off | On | Off |
| 28 | On | On | Off | On | On |
| 29 | On | On | On | Off | Off |
| 30 | On | On | On | Off | On |
| 31 | On | On | On | On | Off |
| 32 | On | On | On | On | On |

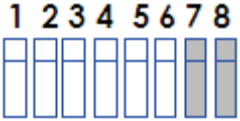
Note

DIP Switch #6 must be set to ON at all times.

### 4.8.2 Tamper Enabling

DIP switches 7 and 8 are used to enable or disable the front and back tamper capability.

**Figure 42: Tamper DIP Switch Setting**




Select the DIP switch setting as described in Table 3 to determine the tamper behavior.

**Table 3: DIP Switch Settings for Tamper Enabling**

| Back | Front | S7 | S8 |
|---|---|---|---|
| **Enabled** | **Enabled** | OFF | OFF |
| **Enabled** | **Disabled** | ON | OFF |
| **Disabled** | **Enabled** | OFF | ON |
| **Disabled** | **Disabled** | ON | ON |

# 5. Communications

The ExpansE system utilizes several communication protocols for the various communication needs.

The MUs are connected to one another via an Ethernet network. This connection also allows access to the web based application used to manage the system.

RS-485 communication protocol is used to connect each MU to its associated EUs.

The EUs address is defined in the ExpansE web application.

It is important that the DIP switch and the software are set to the same address.

# 6. The ExpansE Web Application

ExpansE's built-in Web application and networking capabilities provide faster and easier setup – software installation and computer configuration are not required. The control of all system configuration options and additional services, including real-time monitoring, can be performed from any panel and computer on the network.

Note

For best performance, use either Google Chrome or Mozilla Firefox browsers.

## 6.1 Initial PC Configuration

Before accessing the ExpansE Web application you need to define your PC's IP to match that of the ExpansE's IP.

After Configuring the ExpansE Web application for the first time, remember to revert back to your original IP.

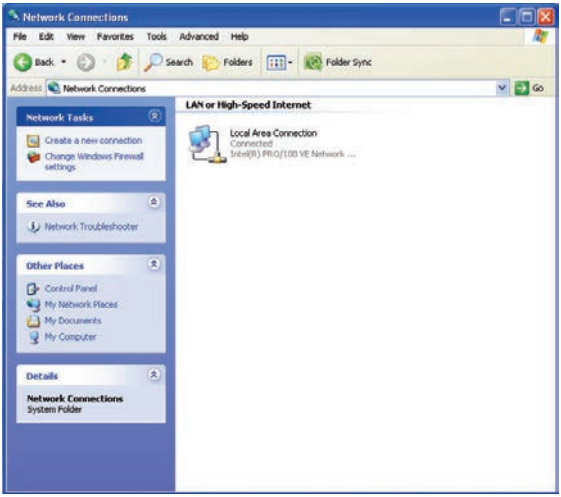
*To define your PC's IP (for Windows XP):*

1. Click **Start > Control Panel** to open the Control Panel.

**Figure 43: Windows XP – Control Panel**

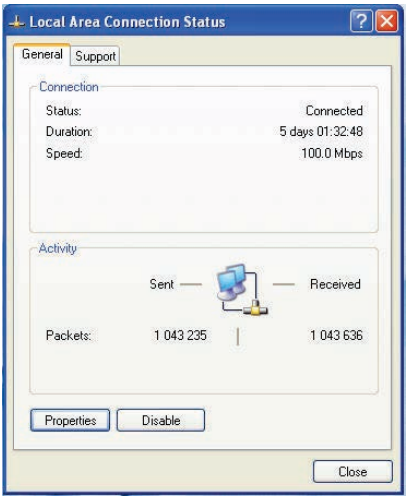
2. Double-click **Network Connections**.
3. The *Network Connections* window opens.

**Figure 44: Windows XP – Network Connections**



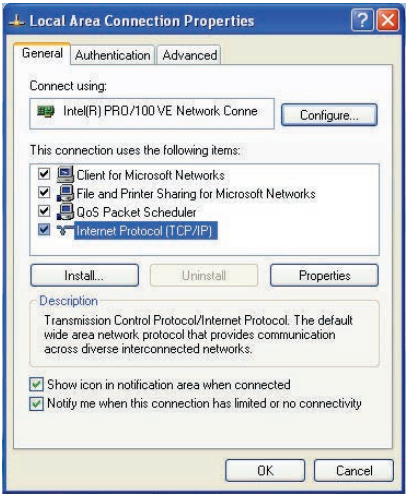

4. Double-click on **Local Area Connection**.
   The *Local Area Connection Status* window opens.

**Figure 45: Windows XP – Local Area Connection Status Window**



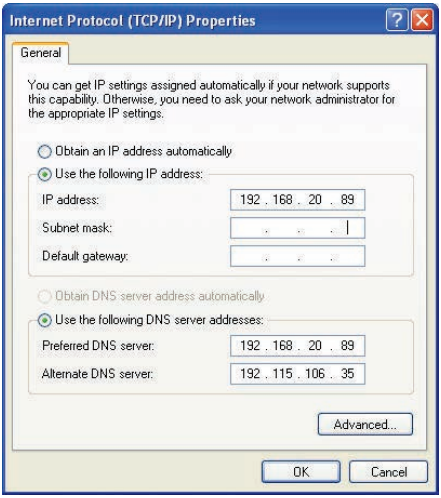

5. Click **Properties** to access the *Local Area Connection Properties* window.

**Figure 46: Windows XP – Local Area Connection Properties Windows**




6. Select Internet Protocol (TCP/IP) and click **Properties**.
   The *Internet Protocol (TCP/IP) Properties* window opens.

**Figure 47: Windows XP – Internet Protocol (TCP/IP) Properties Window**


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 20 . 89
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 20 . 89
Alternate DNS server:
192 . 115 . 106 . 35
Advanced...
OK
Cancel

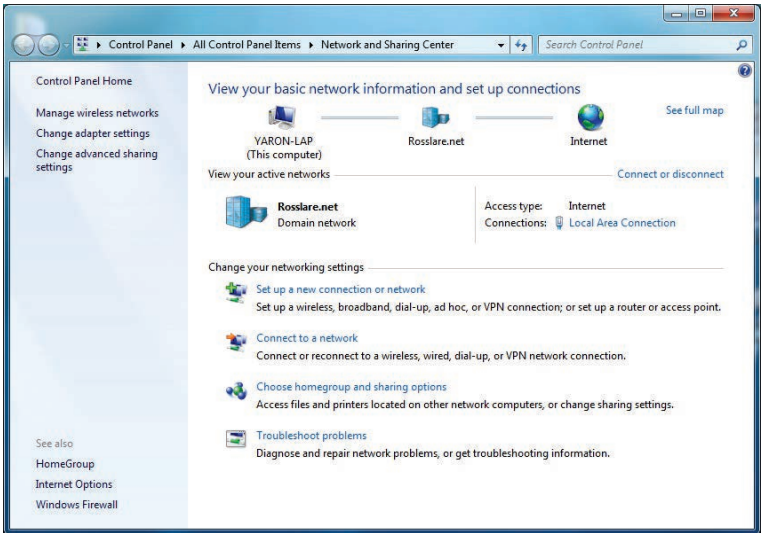
7. Select the **Use the following IP address**:
   a. In the *IP address* field, enter **192.168.20.198**.
   b. In the *Subnet mask* field, enter **255.255.255.0**.
   c. In the *Default gateway* field, enter **192.168.20.1**.

8. Select the **Use the following DNS server address**:
   a. In the *Preferred DNS Server* field, enter **192.168.20.2**.
   b. In the *Alternate DNS Server* field, enter **192.115.106.35**.
9. Click **OK**.
10. After configuring the ExpansE Web application as described in Section 6.2, repeat the process with the correct network settings for your PC as provided by your IT professional.

*To define your PC's IP (for Windows Vista/7):*

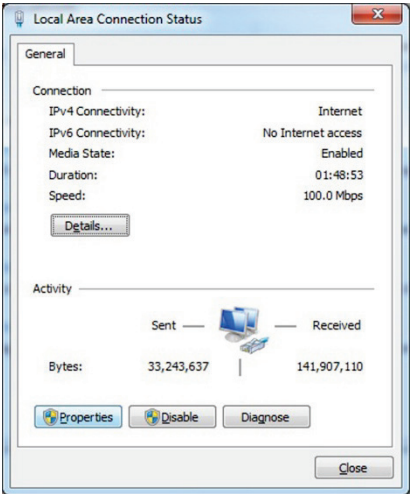
1. Click **Start > Control Panel > Network and Sharing Center** to open the *Network and Sharing Center* window.

**Figure 48: Windows Vista/7 – Network and Sharing Center**


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
YARON-LAP (This computer)
Rosslare.net
Internet
View your active networks
Connect or disconnect
Rosslare.net
Domain network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
HomeGroup
Internet Options
Windows Firewall

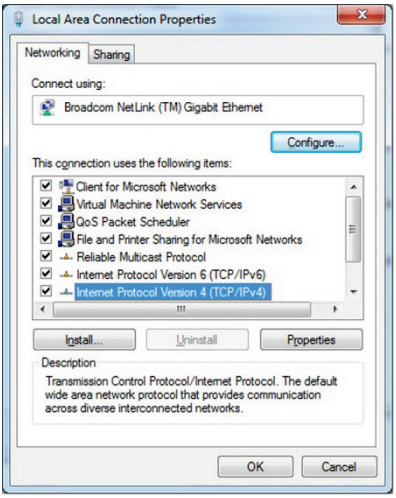
2. Click **Change adapter settings**.
3. Right-click your connection and click **Status**.
   The *Local Area Connection Status* window opens.

**Figure 49: Windows Vista/7 – Local Area Connection Status Window**



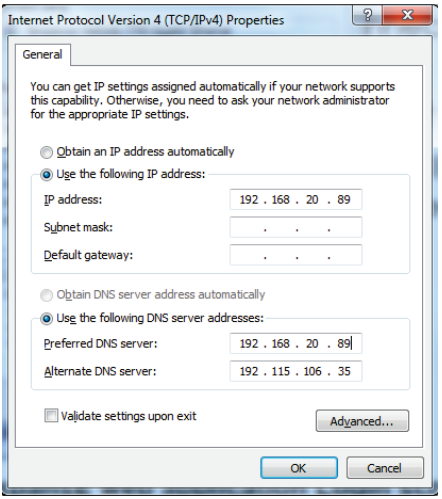

4. Click **Properties** to access the *Local Area Connection Properties* window.

**Figure 50: Windows Vista/7 – Local Area Connection Properties Window**




5. Select Internet Protocol Version 4 (TCP/IPv4) and click **Properties**.
   The *Internet Protocol Version 4 (TCP/IPv4) Properties* window opens.

**Figure 51: Windows XP – Internet Protocol (TCP/IP) Properties Window**


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 20 . 89
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 20 . 89
Alternate DNS server:
192 . 115 . 106 . 35
Validate settings upon exit
Advanced...
OK
Cancel

6. Select the **Use the following IP address**:
   a. In the *IP address* field, enter **192.168.20.198**.
   b. In the *Subnet mask* field, enter **255.255.255.0**.
   c. In the *Default gateway* field, enter **192.168.20.1**.
7. Select the **Use the following DNS server address**:
   a. In the *Preferred DNS Server* field, enter **192.168.20.2**.
   b. In the *Alternate DNS Server* field, enter **192.115.106.35**.
8. Click **OK**.
9. After configuring the ExpansE Web application as described in Section 6.2, repeat the process with the correct network settings for your PC as provided by your IT professional.

## 6.2 Initial Access and Network Settings

The ExpansE web application requires no installation or unique PC setup, any computer connected to the same network as the ExpansE can access the application.

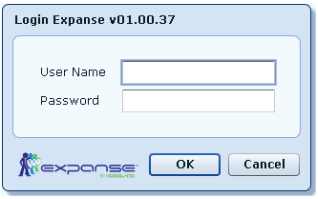
The ExpansE web based application automatically detects and configures connected units, it is therefore crucial that each system (MU and EUs) be connected and defined in the application separately.

*To access and configure the ExpansE for the first time:*

1. Open your web browser and type the default IP address 192.168.20.25 in the address line. The Login screen opens.

> **Note**
> For best performance use either Google Chrome or Mozilla Firefox browsers.

**Figure 52: ExpansE Web Application Login Screen**



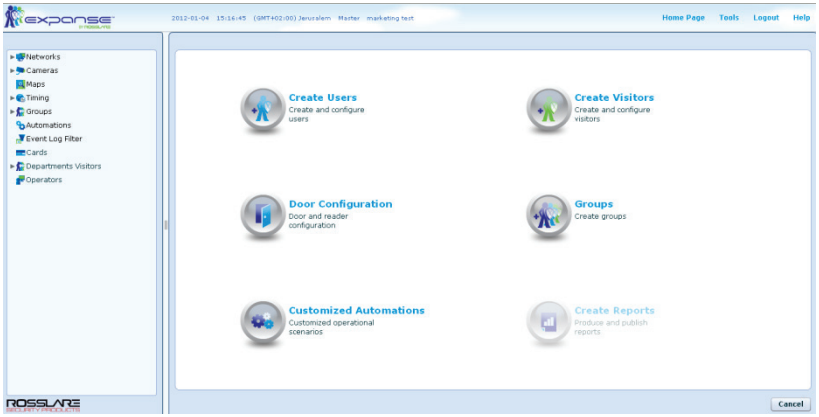

2. Enter your **User name** and **Password**.

> **Note**
> By default, the user name and the initial password is Admin. Enter "admin" in the **User name** and **Password** fields.

3. Click **OK**.

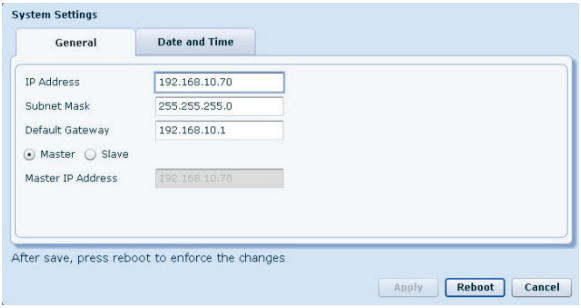
   The ExpansE home window opens (see Figure 53), followed immediately by the settings window (see Figure 54 and Figure 55).

**Figure 53: ExpansE Web Application Homepage**




4. When accessing the application for the first time, the system settings window opens automatically to configure the system. The same window can be accessed using the **Tools>Settings** link located on the main window's upper right corner.

**Figure 54: System Settings – General Tab**



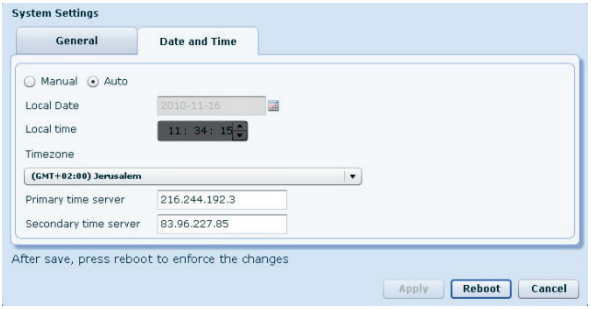

5. Ensure that the *Master* option is selected; any additional MUs that are defined in the system are defined as *Slaves*.
6. Define the ExpansE's network identity.

Contact your network administrator for assistance in finding the network parameters needed.

   a. Set the *IP Address* for the ExpansE MU.
   b. Set the *Subnet Mask* for the ExpansE MU.
   c. Set the *Default Gateway* for the ExpansE MU.
   d. When defining slave MUs, enter the IP Address of the master MU in the *Master IP* Address field.
   e. Click the **Date and Time** tab to continue with the initial configuration.
7. Set your Date and Time:
   a. Ensure that ***Auto*** option is selected and select your time zone from the *Timezone* list.

      The time and date are automatically updated from either the Primary or Secondary time server.

**Figure 55: System Settings – Date and Time Tab**



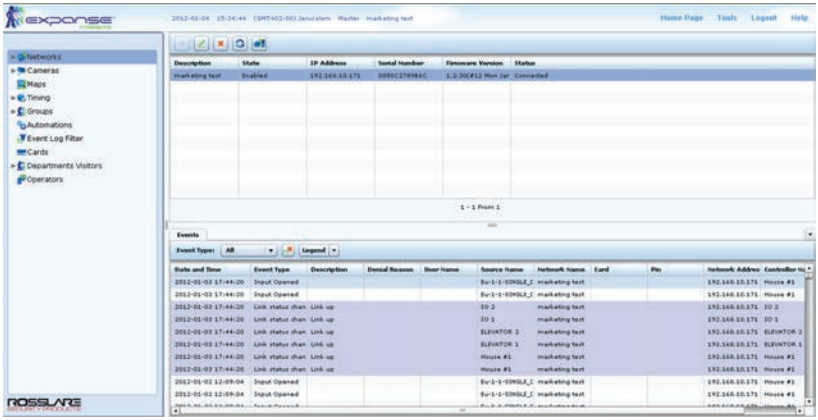
b. Select the Manual option to define the date and time.
   i. Enter the date in the *Local Date* field or open the calendar by clicking the calendar icon and select the date.
   ii. Enter a time or use the arrows to set the time in the *Local Time* field

8. Click **Apply** to save the changes made.
9. Click **Reboot** to restart the unit and implement the changes in the MU.

## 6.3 The ExpansE Main Window

The entire central functionality of the ExpansE web-based application is available from its main window.

**Figure 56: ExpansE Web Application Main Screen**



The ExpansE web application's main window is divided into the following sections:

| Section | Description |
|---|---|
| **Display Area (1)** | Displays all items within the tree view selected element. |
| **Tree View (2)** | Allows users to configure, monitor, and control every aspect of the ExpansE system. For more information, see Section 6.4. |
| **Toolbar (3)** | Has toolbar icons which users can use for the key tasks required in managing access control across a facility. The available icons change according to the view selected. For more information, see Section 6.5. |
| **Menu Bar (4)** | Controls the software general operation and setup. For more information, see Section 6.6. |
| **Event Window (5)** | Displays 200 events comprised of general status information, such as: Operator name, Client/Server mode, system readiness, system download, date, and time. |

## 6.4 Tree View

The Tree View allows users to configure, monitor, and control every aspect of a facility's access control network. When the user selects an element from the tree, its content is shown in the main display area.

### 6.4.1 Networks

A network is a group of MUs each with up to 32 EUs. The ExpansE connects to the units across the Ethernet between MUs and RS-485 between EUs. The ExpansE system automatically detects and configures connected units, you only need to initialize it in the system. For more information, see Section 7.1.

### 6.4.2 Cameras

The Cameras element lists the camera connected to the network and their statuses (see Section 7.6). In addition, if the ExClouds application is installed, you can view each camera's live stream (see Section 10.2).

### 6.4.3 Maps

The Status Map displays the status of every door, reader, and alarm in the facility on user-selected floor plans.

The system can display multiple nested status maps, allowing users to show either the complete access control network or a specific area in detail.

### 6.4.4 Timing

Timing defines a weekly time period or set of time periods, for example, "Office Hours" or "Out of Office Hours". Door access rights, alarms, and input/output behavior can all be set to behave differently within each Timing set. For more information, see Section 7.8.

### 6.4.5 Groups

Groups consist of access groups, input groups, output groups and elevator groups. An Access Group defines when each reader on the site is available for access. All site personnel are assigned to appropriate Access Groups. See Section 7.9.

Input and Output groups define sets of outputs or inputs that should be managed together within a panel. See Section 7.5.

Elevator groups are similar to output groups but are dedicated to elevator control EUs and application. See Section 7.12.

### 6.4.6 Automation

The Automation element defines automated activities based on various input and output settings as well as other variables such as events and time zones (see Section 7.13).

### 6.4.7 Event Log Filter

The Events Log Filter allows you to define the type of events that are displayed and saved in the log file by selecting those you wish to exclude (see Section 7.17).

### 6.4.8 Cards

The Cards element lists all cards in the system and their statuses, and allows manual or automatic card addition to the system (see Section 7.14).

### 6.4.9 Departments and Visitors

This element lists all departments and users, as well as visitors. Each user is a member of a department. For each user, it is possible to assign a card and/or a PIN code, set access rights, personal details, and include an identification photograph. The setup also allows you to create visitors with their specific associated rights. See Section 7.15.

### 6.4.10 Operators

Operators are users with access privileges to the ExpansE web application. Different operators can be defined to have broader or more restricted security privileges, from complete control over the system to the ability only to view one section. All Operator passwords are case-sensitive.

Only one operator with full administrator privileges can access the system simultaneously; other administrators trying to log in only have read rights during that time.

Up to 20 users with read only privileges can access the system at the same time.

## 6.5 Toolbar

The toolbar controls key tasks required to manage access control across a facility.

The following toolbar icons are available:

### 6.5.1 General Icons

| Icon | Name | Click icon to... |
|---|---|---|
| | **Open Door Manually** | Open the Door Manual Operation window (see Section 9.1) |
| | **New** | Create a new element of the selected type |
| | **Edit** | Edit the selected element |
| | **Delete** | Delete the selected item |
| | **Refresh** | Refreshes the current view |
| | **Reader Manual Options** | Open the Reader Manual Operation window (see Section 9.2) |
| | **Output Manual Options** | Open the Output Manual Operation window (see Section 9.3) |

### 6.5.2 Event Type Icon

| Icon | Name | Click icon to... |
|---|---|---|
| | **Clear All Events** | Clears all displayed Events. Click the dropdown arrow to change the view. The event are not erased and are shown the next time you log in. |

## 6.6 Menu Bar

The menu bar controls the general operation and setup of the application.

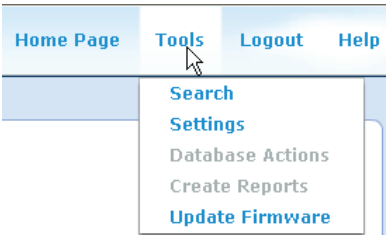
### 6.6.1 Home Page

**Home Page** contains several configuration wizards. See Chapter 8.

### 6.6.2 Tools

The *Tools* menu contains five submenus, as seen in Figure 57.

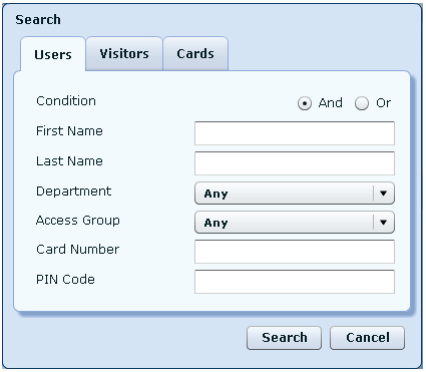
**Figure 57: Tools Menu**




#### 6.6.2.1 Search

The *Search* window under the *Tools* menu consists of three tabs: User, Visitor, and Card (Figure 58).

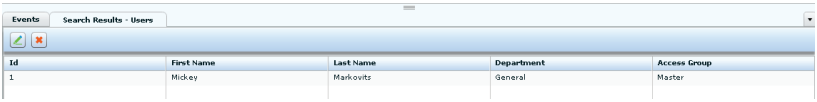
**Figure 58: Search Option**




In each of the tabs, you can enter various parameters to narrow your search.

The search results are then displayed in a tab next to the Events tab in the Event Window area.

**Figure 59: Search Results Tab**




6.6.2.2 Settings

See Steps 4 to 9 in Section 6.2 on how to set/change the system settings.

6.6.2.3 Update Firmware

You can update the firmware of various EUs as needed.

See Chapter 12 for details.

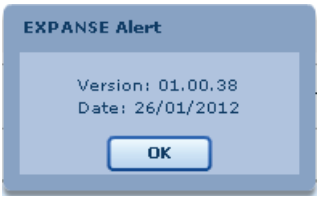
### 6.6.3 Logout

Clicking **Logout** logs you out of the system. For security and management reasons only one operator with administrative rights can be logged in at one time.

### 6.6.4 Help Menu

The help menu opens the *About* screen, which shows the system information.

**Figure 60: ExpansE Web Application About Screen**




## 6.7 Event Log

Every time access is granted or denied, for every door on a site an entry appears in the log file which is part of the static view of the ExpansE main window. Monitoring for potential door tampering or forced entry is logged, and displays of internal system warnings are also shown.

The events shown are defined in the *Event Log Filter* window (see Section 7.17).

You can also filter the view for a specific session using the even filter drop down list and clear the even logs shown using the clear all Icon on the event log tool bar.

# 7. How to Set Up a Site

This section outlines a recommended step-by-step process for configuring the ExpansE system.

| Step | Action | Section |
|---|---|---|
| **01** | **Setting a Controller (MU)** | 7.1 |
| **02** | **Configure the various associated EUs** | 7.2 through 7.5 |
| **03** | **Add cameras** | 7.6 |
| **04** | **Add overview maps** | 7.7 |
| **05** | **Add time zones and holidays** | 7.8 |
| **06** | **Add access groups** | 7.9 |
| **07** | **Add input groups** | 7.10 |
| **08** | **Add output groups** | 7.11 |
| **09** | **Add elevator groups** | 7.12 |
| **10** | **Add automation behavior** | 7.13 |
| **11** | **Add cards** | 7.14 |
| **12** | **Add departments and users** | 7.15 |
| **13** | **Add visitors** | 7.16 |

## 7.1 Setting a Controller (MU)

The ExpansE network is set up of a master MU with several slave MUs, each with a network of EUs.

Each MU is automatically detected and configured but need to be initialized.

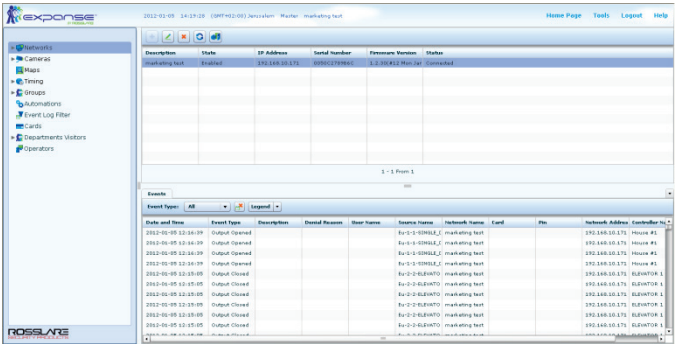
Note

It is crucial that each subsystem (MU and EUs) be connected and defined in the application separately.

*To define the MU settings:*

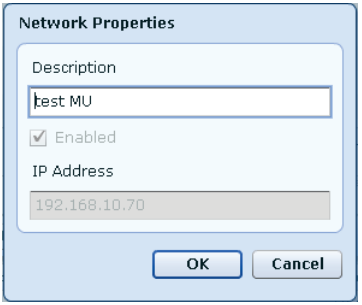
1. In the tree view, select **Networks**.

**Figure 61: ExpansE Web Application Networks Screen**



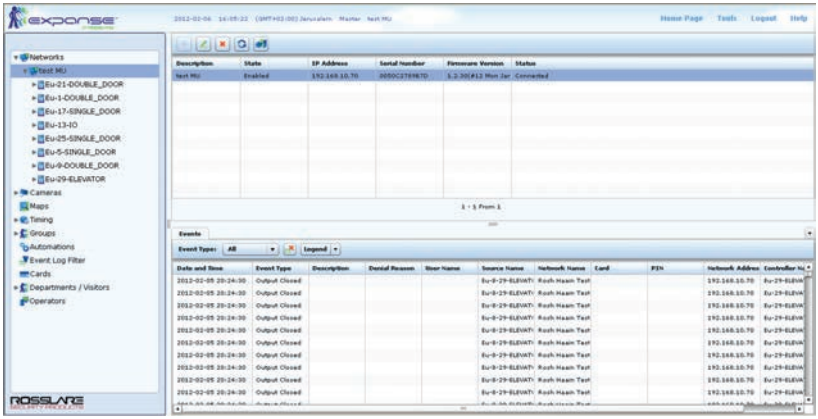
2. From the list of networks, select an MU and click the **Edit** icon.
   The *Network Properties* window of that MU opens.

**Figure 62: Network Properties Window**




3. Enter a description for the MU in the **Description** field
4. Select the **Enabled** checkbox to enable the MU.
5. Click **OK**.
   The connected EUs appear in the tree view.

**Figure 63: Networks Screen with Connected EUs**



6. Select an EU and click the **Edit** icon to open the EU Properties window.
7. Enter a description for the EU in the **Description** field.
8. Select the **Enabled** checkbox, to enable the EU.
9. Click **OK**.

## 7.2 Configuring Doors

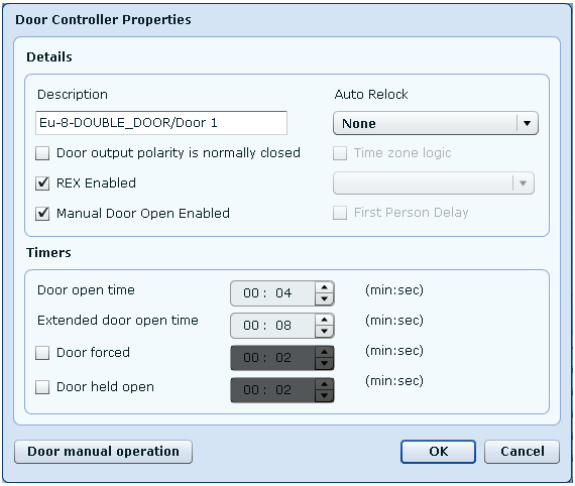
Each Door Controller controls one or two doors as well as inputs and outputs, each door can be configured individually.

Set the properties for each of the doors.

*To set door properties:*

1. In the tree view, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.
3. Select a door to set its properties.
4. Click the **Edit** icon.
   The *Door Controller Properties* window opens.

**Figure 64: Door Controller Properties Window**




5. In the **Description** field, enter a name for the door.
6. From the **Auto Relock** select box, select the event that causes the door to relock automatically
7. Determine the door polarity by selecting or clearing the **Door output polarity is Normally Closed** checkbox.

   Select this checkbox to ensure Fail Safe door opening if the Fail Safe door Lock Device power fails.

   Once enabled, the door output relay is activated when the door is closed, and is deactivated when the door is open.

   In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals
8. Select the **REX enabled** checkbox to allow Requests to Exit for this door.
9. Select the **Manual Door Open Enabled** checkbox to allow operators to adjust the door manually (see Section 9.1).
10. Sets the door's time zone logic behavior.
    a. Select the **Timezone Logic** checkbox to initiate the time zone logic options and select an output from the list.
    b. Select the **First person Delay** checkbox to keep the door locked until the first user opens it.
11. Set the duration for which the door stays unlocked by typing minutes and seconds in the **Door open time** field or use the associated up and down arrows.

12. Set the duration for which the door stays unlocked for users with Extended door open rights by typing minutes and seconds in the **Extended Door open time** field or use the associated up and down arrows.
13. Set the duration following which and when the door is forced open, an event occurs.
14. Select the **Door forced** checkbox to use this timer.
15. Enter the minutes and seconds in the associated field or use the up and down arrows.
16. Set the duration for which the door can be held open without raising an alarm event.
17. Select the **Door held open** checkbox to use this timer and enter the minutes and seconds in the associated field or use the up/down arrows.
18. Click **OK**.

## 7.3 Setting a 16-Relay Elevator Control Unit

A 16-Relay Elevator Control Unit has 16 outputs and is associated to inputs in order to activate these outputs

Set the properties for each of the inputs and outputs for each of the elevator control EU's.

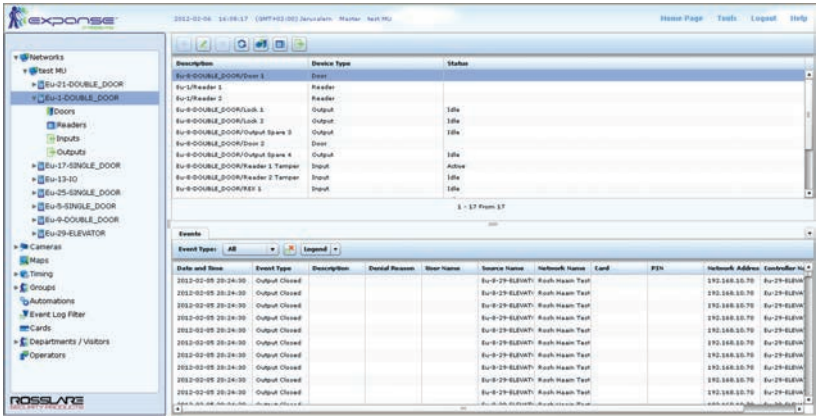
*To set the 16-relay elevator control unit properties:*

1. In the tree view, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.

   Select an elevator control EU to set its properties.
3. Define the inputs and outputs as explained in the Section 7.5.

**Figure 65: Elevator Control EU Window**



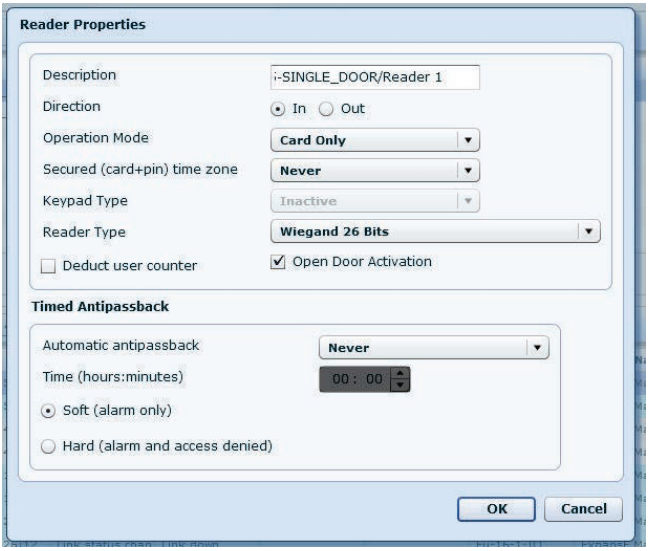
## 7.4 Configuring Readers

Each Dual Reader Door Unit can be connected to one or two readers.

*To configure a reader:*

1. In the Tree View, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand the tree view.
3. Select a Dual Reader Door Unit and expand the tree view.
4. Select a reader to set its properties.
5. Click the **Edit** icon.
   The *Reader Properties* Window opens.

**Figure 66: Reader Properties Window**




6. Select whether and when to apply antipassback rules from the **Automatic antipassback** list.
7. Set the time when to apply antipassback rules by typing hours and minutes in the **Time (Hours:Minutes)** field or use the associated up and down arrows.
8. Select either **Hard** or **Soft** antipassback application.
   When hard antipassback is selected, an event is generated and the door does not open.
   When soft antipassback is selected, the door opens but an event is generated.
9. In the **Description** field, enter a name for the reader.

10. Select whether the reader is allowing entry into the area or exit out of the area by selecting either the **In** or **Out** option.
11. From the Operation Mode list, select how the reader operates:
    - **Inactive:** The reader is not in use.
    - **Card Only:** The reader accepts RFID cards only.
    - **PIN Only:** The reader accepts PIN inputs only.
    - **Card or PIN:** The reader accepts both cards and PIN codes.
    - **Card and PIN:** Higher security – The reader requires both cards and PIN code for access.
    - **Desktop:** The reader is inactive, but is being used to record new cards on the computer.
    - **No Access Mode:** The reader grants access to no users.
12. Using the **Secured (Card+PIN) time zone** list select a time zone during which access should be granted only after both the card and PIN are entered.

    The PIN must be entered within 10 seconds of card entry.
13. From the **Keypad Type** list, select the data transmission type for the type of keypad hardware.
14. From the **Reader Type** list, select the data transmission type for the reader hardware.
15. Select the **Biometric Reader** checkbox to allow use of Rosslare's biometric readers.
16. Select the **Deduct User Counter** checkbox to record this entry against the user's entry allowance counter.
17. Select the **Open Door Activation** checkbox to allow the reader to unlock the door.
18. Click **OK**.

## 7.5 Configuring Inputs and Outputs

Inputs and outputs are available in each of the EUs. The number of Inputs and outputs depends on the type of EU.

*To configure inputs and outputs:*

1. In the Tree View, click **Networks**.

   The available networks are listed in the display area.
2. Select a network and expand the tree view.
3. Select one of the available EUs and expand the tree view.
4. Select an input to set its properties.
5. Click the **Edit** icon.

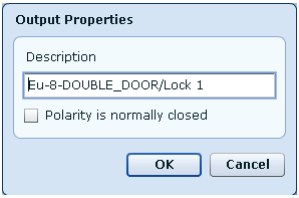
   The *Input Properties* window opens.

**Figure 67: Input Properties Window**

6. In the **Description** field, enter a name for the input.
7. From the **Property** field select the type of input to be monitored.
   - **Normally Open/Close:** An input either in an open or closed state.
   - **Normally Open/Close 1 Resistor:** An input in an open, closed, or trouble state. This option is only available for supervised inputs.
   - **Normally Open/Close 2 Resistors:** An input in an open, closed, or trouble state, with additional checks for short-circuit and open-circuit tampering. This option is only available for supervised inputs.
8. Enter the minutes and seconds in the **Start Delay** field or use the up and down arrows to set the delay time before this input becomes active. Note that on normally open input, the delay starts once the input contact is closed. On normally closed input, the delay starts once the input contact opens.
9. Click **OK**.
10. Select an output to set its properties.
11. Click the **Edit** icon.

    The *Output Properties* window opens.

**Figure 68: Output Properties Window**




12. In the **Description** field, enter a name for the output.
13. Click **OK**.

## 7.6 Adding Cameras

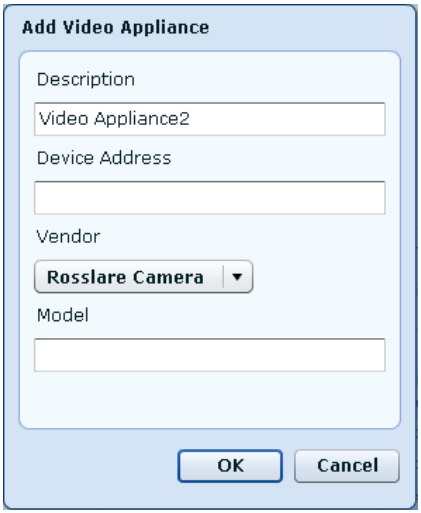
Cameras can be added to the network to allow real-time viewing of any area desired. The Camera element allows you to add cameras to the network and to configure each camera's setting.

If you wish to view the live stream of a camera, the ExClouds application must be installed (see Section 10.2).

*To add a camera:*

1. In the Tree View, select **Cameras**.
2. Click the icon.
   The *Add Video Appliance* window opens.

**Figure 69: Add Video Appliance Window**




3. In the **Description** field, enter a name for the camera.
4. Add the IP address of the device.
5. [Optional] Select the camera vendor from the dropdown.
6. [Optional] Enter the model of the camera.
7. Click **OK**.

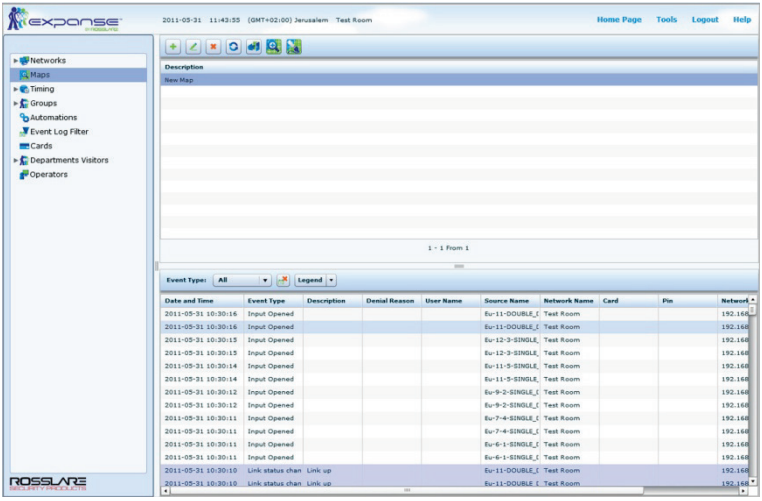
## 7.7 Adding Active Maps

The Status Map displays the every enrolled unit in the system along with status indications for every door, input, output, antipassback rules, and alarms in the facility. The statuses are shown overlaid on a user-selected image such as floor plans, satellite image, and so on.

*To create a status map:*

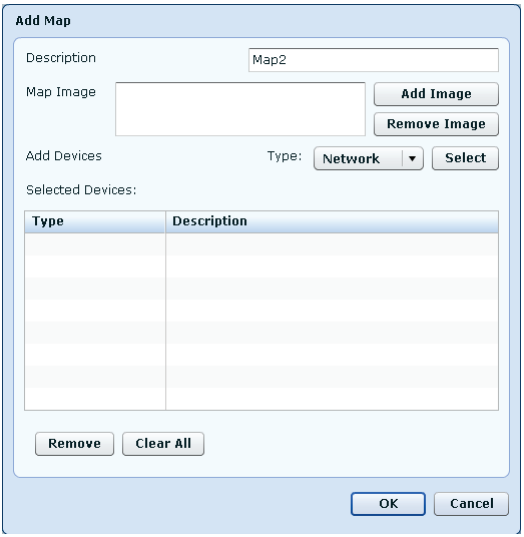
1. In the tree view, click **Maps**.
   The map management screen appears.

**Figure 70: Map Management Screen**




2. Click the icon.
   The *Add Map* window opens.

**Figure 71: Map Properties Window**



3. Enter a name for the map in the **Description** field.
4. Click **Add Image** to select the image to be used in the map.
   The *Select Image* window opens.

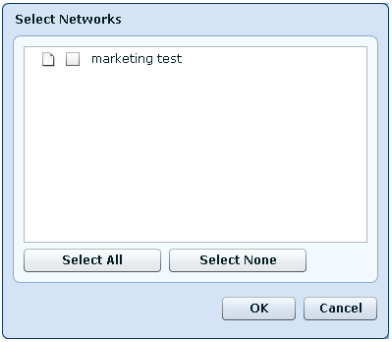
**Figure 72: Select Image Window**

Note

The image files are taken from the MU's USB flash drive, the MU cannot import images and files from remote disk drivers.

5. Select a graphic file for the Status Map background.
6. Click **OK**.
   The file selected is shown in the Map Image field.
   The files types supported are one of the following formats: jpg, gif, or bmp.
7. Add Networks to the map:
   a. In the **Type** select box, select ***Network*** and click **Select**.
      The *Select Networks* window opens.

**Figure 73: Select Networks Window**



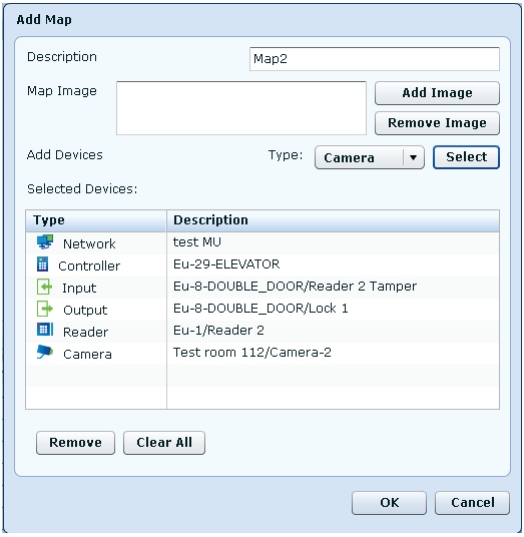
b. Select one or more networks from the list of available networks.

You can also click **Select All** to select all of the available networks or **Select None** to deselect all of the networks.

c. Click **OK**.

The device selected appears in the Selected Devices field.

**Figure 74: Map Properties Window with Devices**




d. Repeat the process for Controllers, Doors, Readers, Inputs, outputs, panels, and so on.

8. To remove devices from the list, select a device in the selected devices field and click **Remove**. To remove all of the devices click **Clear All**.

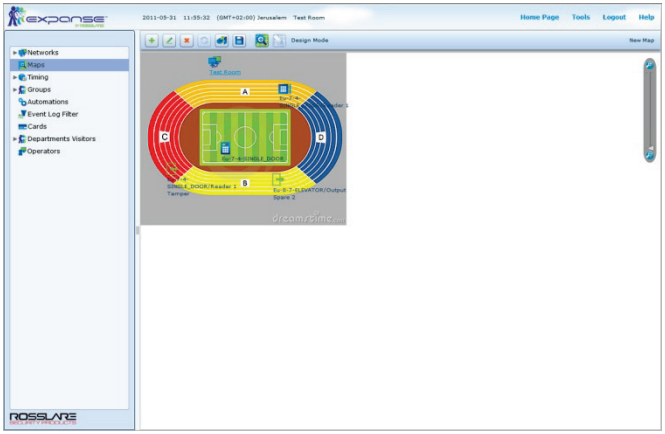
   Click **OK** to return to the map management window.

9. Click the **Design** icon to enter design mode.

Note

It is highly recommended to add devices and place them in the design mode in batches to avoid clutter in large installations.

**Figure 75: Map Design Mode**



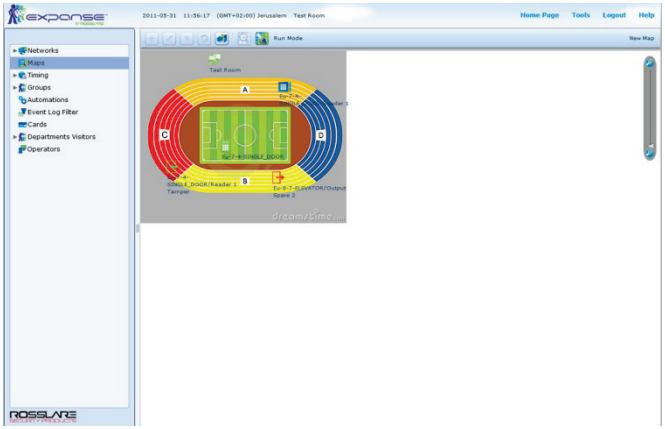

The objects appear on the status map.

10. Drag each device to its correct position.

> **Note**
>
> Status map icons can also be added to other status maps, indicating where the two map areas meet.

11. Click the **Show Map** icon to enter Run mode.

**Figure 76: Map Run Mode**



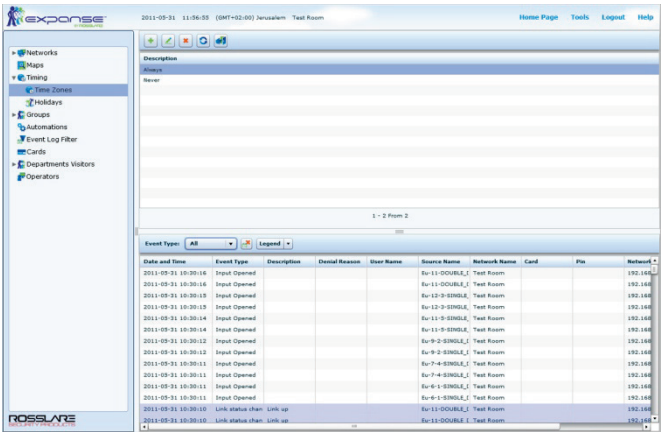
## 7.8 Adding Time Zones and Holidays

Timing refers to a group of time periods within a week. Door access rights, as well as input and output behavior, can all be set to behave differently for each time zone. Many operations can be automatically enabled or disabled within a selected time zone.

*To set a new time zone:*

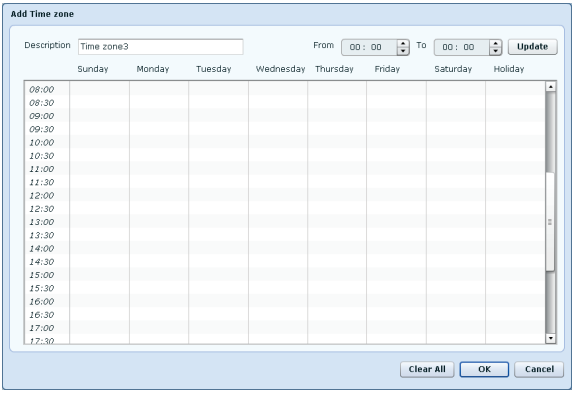
1. In the tree view, select **Timing** and then **Time Zones**.

**Figure 77: Timing Window**




2. On the toolbar, click the icon.
   The *Add Time Zone* window opens.

**Figure 78: Add Time Zone Window**

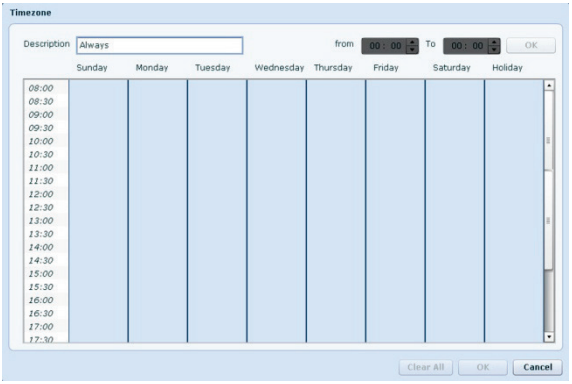



3. In the **Description** field, enter a name for the time zone.

4. Select the days for which the time period is within the time zone by clicking anywhere in those days. The "Holiday" day can be set to include national holidays.
5. Set the start and end time of the time zone typing hours and minutes in the **From** and **To** fields or use the associated up and down arrows.
6. Click **Update** to apply your changes.
7. Click **OK**.

   The window closes and the display area displays the new time zone.

**Figure 79: Time Zone Window**




8. In the tree view, select **Timing** and then **Holidays**.
9. On the toolbar, click the icon.

   The *Add Holiday* window opens.

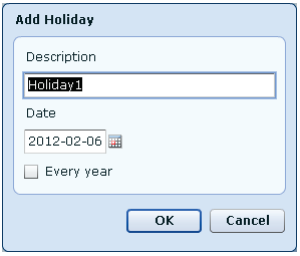



**Figure 80: Holiday Properties Window**

10. In the **Description** field, enter a name for the holiday.
11. Enter the holiday's date in the ***Date*** field or open the calendar by clicking the calendar icon and select the date.
12. Select the **Every Year** checkbox to repeat the holiday on a yearly basis on the same date.
13. Click **OK**.

## 7.9 Adding Access Groups

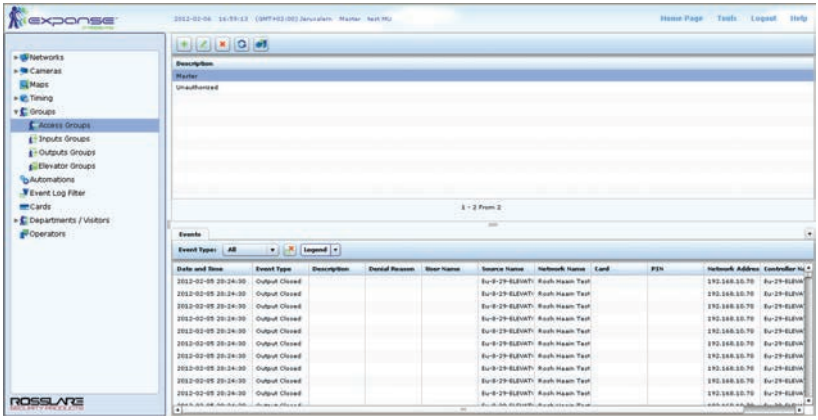
An access group includes a list of door readers and the time zones during which each of those door readers are available for access. Every user is assigned to an access group.

The *Access Group* window lists all the door readers defined in the database, and the time zones during which they can be accessed.

*To create an access group:*

1. In the Tree View, expand the **Groups** element and select **Access Groups**.

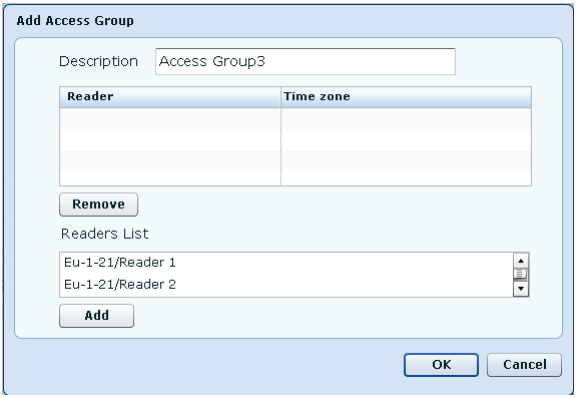
**Figure 81: Access Group Window**




2. On the toolbar, click the icon.

   The *Add Access Group* window opens.

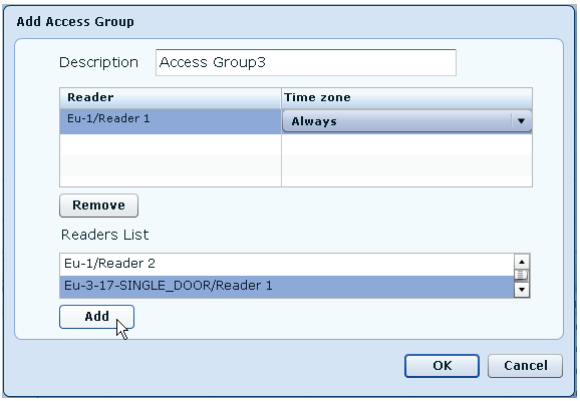
**Figure 82: Access Group Properties Window**




3. In the **Description** field, enter a name for the access group.

4. From the *Readers List*, select the readers you wish to associate with this group and click **Add**.

**Figure 83: Add Access Group Window with Associated Readers**




5. For each of the readers select a time zone association.
6. Click **OK**.

## 7.10 Adding Input Groups

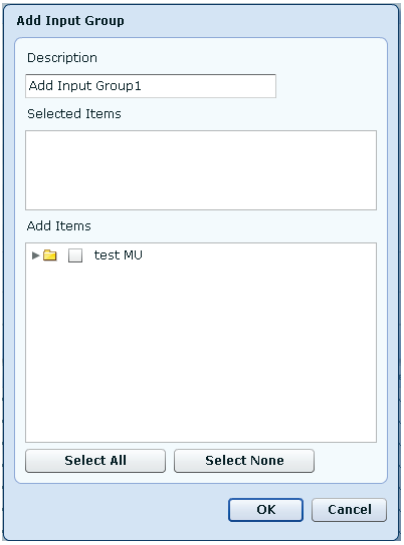
Input groups are a collection of Inputs from one or more panels that can be used in panel links to perform advanced operations.

*To set an Input Group:*

1. In the Tree View, expand the **Groups** element and select **Input Groups**.
2. Click the icon.

   The *Add Input Group* window opens.

**Figure 84: Add Input Group Window**




3. In the **Description** field, enter a name for the input group.
4. Within *Add Items,* select all the inputs you wish to add.

   You can also click **Select All** to select all of the available inputs or **Select None** to deselect all of the inputs.
5. Click **OK**.

   All of the associated inputs are shown in the *Selected Items* section.

## 7.11 Adding Output Groups

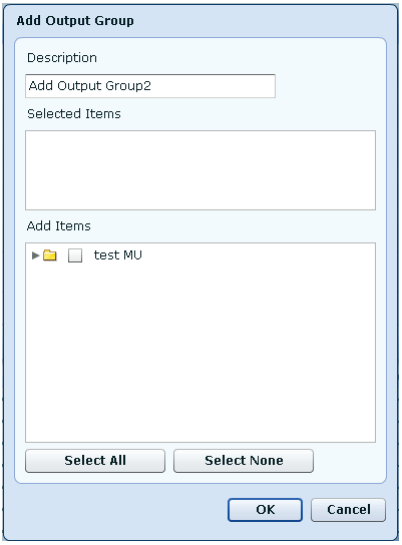
Output groups are a collection of Outputs from panel or panels that can be used in panel links to perform advanced operations.

### *To add an Output Group*

1. In the Tree View, expand the **Groups** element and select **Output Groups**.
2. Click the icon.

   The *Add Output Group* window opens.

**Figure 85: Output Group Window**




3. In the **Description** field, enter a name for the output group.
4. Within *Add Items*, select all the outputs you wish to add.
5. You can also click **Select All** to select all of the available outputs or **Select None** to deselect all of the outputs.
6. Click **OK**.

   All of the associated outputs are shown in the *Selected Items* section.

## 7.12 Adding Elevator Groups

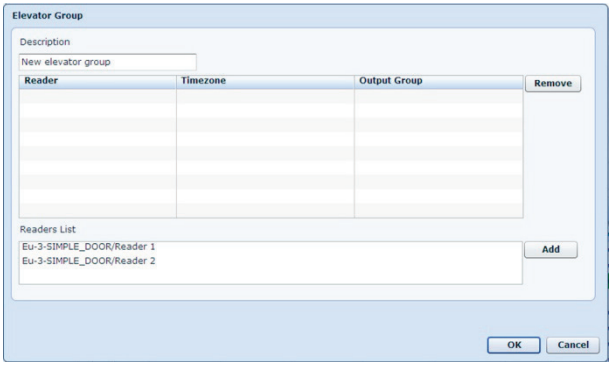
Elevator groups are a collection of inputs and outputs from various EUs that can be linked to perform advanced operations, such as Elevator control.

### *To set an Elevator Group*

1. In the Tree View, expand the **Groups** element and select **Elevator Groups**.
2. Click the icon.

   The *Elevator Group* window opens.

**Figure 86: Output Group Window**




3. In the **Description** field, enter a name for the elevator group.
4. In the *Reader List* section select all the readers you wish to add to the group.

   All of the associated readers are shown in the list.
5. For each of the selected readers select an associated **Time zone** and **Output Group**.
6. Click **OK**.

## 7.13 Adding Automation

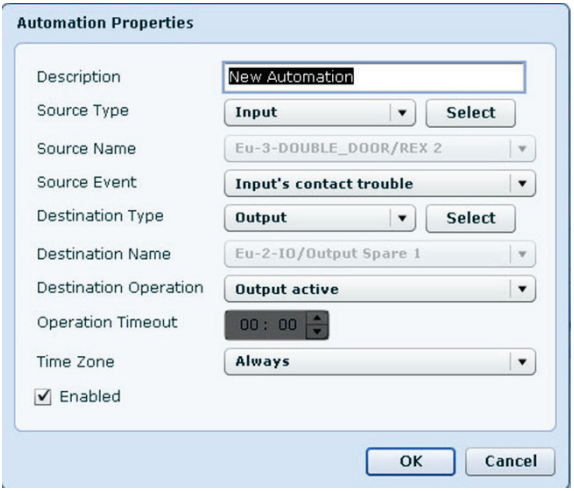
Set various automated applications by associating various input and reader events with various output actions.

*To define various automatic operations:*

1. In the Tree View, expand the **Automation** element.
2. Click the icon.

   The Automation Properties window opens.

**Figure 87: Automation Properties Window**




3. In the **Description** field, enter a name for the automated activity.
4. From the **Source Type** list, select the desired source and click **Select**.
5. From the **Source Name** list, select the specific source. This select box is only available after you selected a source type.
6. Based on the source selected various events are shown in the **Source Event** list, select the event you wish to use.
7. From the **Destination Type** list, select the desired output type and click **Select**.
8. From the **Destination Name** list, select the specific output. This select box is only available after you selected a destination type.
9. Based on the output selected various operations are shown in the **Destination Operation** list, select the operation you wish to perform.
10. Enter the minutes and seconds in the **Operation Timeout** field or use the up and down arrows to set the time frame for the operation timeout.
11. Select a time zone for this operation from the **Time Zone** list.
12. Select the **Enable** checkbox to enable the automated operation.
13. Click **OK**.

## 7.14 Adding Cards

The ExpansE Web Based application database maintains a list of every user card or PIN that has ever been assigned. The Add Cards window defines:

- The type of reader needed to read the card
- The number of cards to create

*To define cards:*

1. In the Tree View, select **Cards**.
2. On the toolbar, click the icon.
   The *Add Cards* window opens.

**Figure 88: Add Cards Window**

3. From the **Reader Type** list, select the type of reader appropriate for the cards being enrolled.
4. In the **Cards Quantity** field, enter the number of cards to add.
5. Enter the number of the first card in the set in the **Start From** field.
6. Set the **Facility Code** as required, and then click **OK**.
   A dialog reports that the operation has been completed.

## 7.15 Adding Departments and Users

Every user is grouped within a department. The ExpansE web based application stores contact details for each user, associated card details, and user access rights.

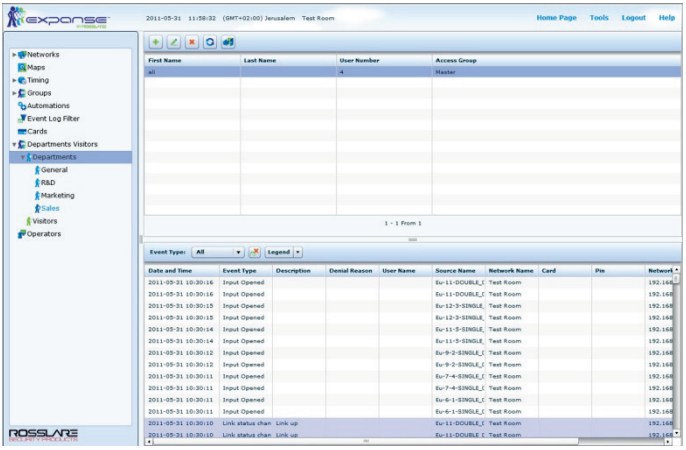
The User Properties window has three tabs:

- General tab displays identification and control information
- Details tab records user contact details
- Codes tab displays information about cards associated with the user

*To create departments:*

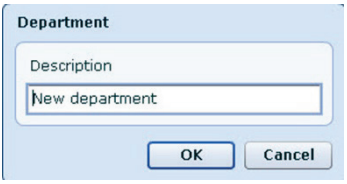
1. In the tree view, expand the *Departments Visitors* element and select **Departments**.

**Figure 89: Departments/Users/Visitors Window**




2. To create a new Department, click the icon.
   The **Department** dialog opens.

**Figure 90: Department Dialog**

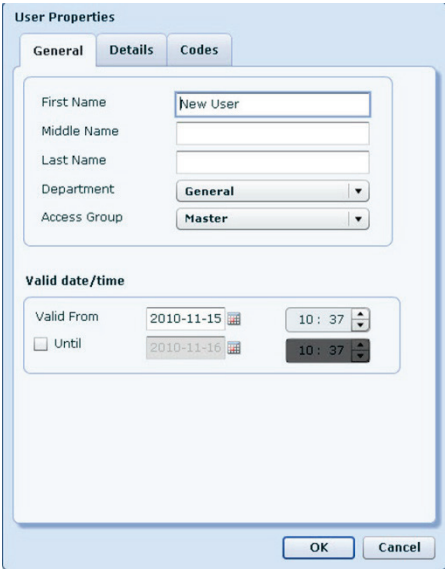



3. Enter a name for the department and then click **OK**.

*To create users:*

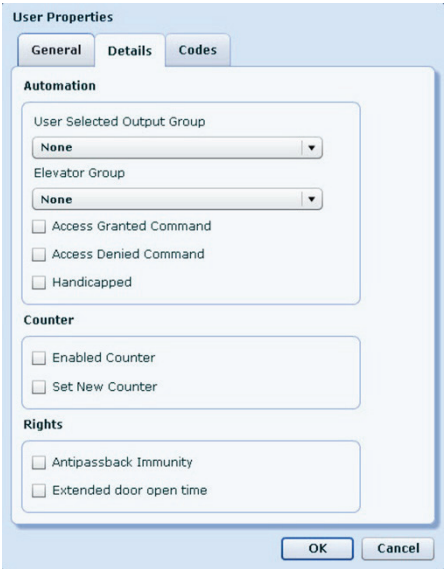
1. In the tree view, expand the *Departments Visitors* element.
2. Select a department and click the icon.
   The *User Properties* window opens in the General tab.

**Figure 91: User Properties Window – General Tab**



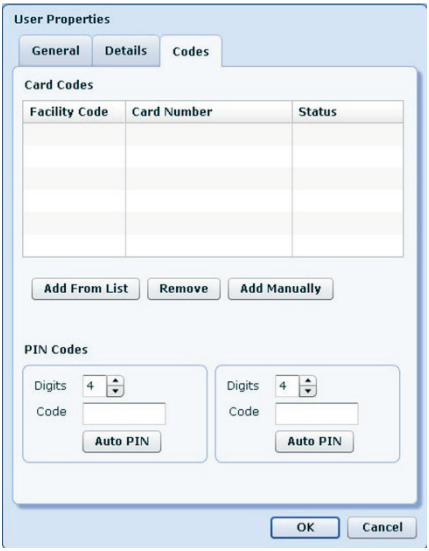

3. Enter the user's first name in the **First Name** field.
4. Enter the user's middle name in the **Middle Name** field.
5. Enter the user's last name in the **Last Name** field.
6. From the **Department** Select box, associate the user with one of the departments you created.
7. From the **Access Group** Select box, associate the user with an access group.
8. Set the access validity date and time. For limited access rights, select the **Until** checkbox and set the final date and time.
9. Click the *Details* tab to continue.

**Figure 92: User Properties Window – Details Tab**




10. Set the Automation options:
    a. Select an output group previously created from the **User Selected Output Group** dropdown.
    b. Select an Elevator group previously created from the **Elevator Group** dropdown.
    c. Select the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
    d. Select the **Handicapped** checkbox to set handicapped privileges.
11. Set the counter options:
    a. Select the **Enable Counter** checkbox to activate.
    b. Select the **Set New Counter** checkbox to reset.
12. Set the access right options:
    a. Select the **Antipassback Immunity** checkbox to override any antipassback restrictions for this user.
    b. Select the **Extended door open time** checkbox to allow this user extended unlocked door duration. The extended duration is set for each door.
13. Click the *Codes* tab to continue.

**Figure 93: User Properties Window – Codes Tab**




14. Set the card associated to the user; you have one of several options to do so:
    a. Click the **Add From List** button to select a card already added to the system.
    b. Select a card from the list shown and click the **Remove** button to remove the card associated to the user.
    c. Click the **Add Manually** button to type the card number then click the **Add From List** button to associate it with the user.
15. Define one or two PIN codes associated with the user:
    a. Define the length of the PIN for this user – enter a value or use the arrows in the **Digits** text box.
    b. Enter a PIN number based on the length defined in one or both of the **Code** text boxes.
    c. Click the **Auto PIN** button to automatically generate a random PIN.
16. Click **OK**.

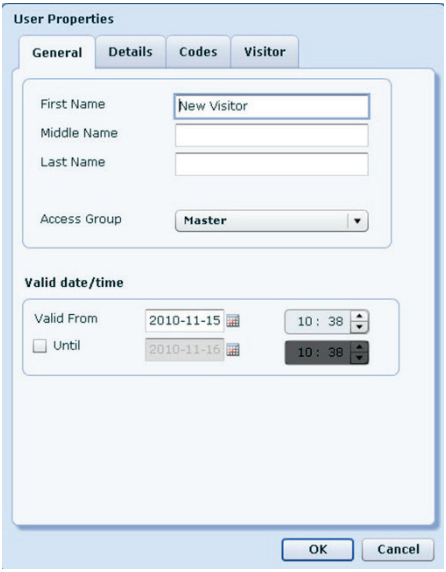
## 7.16 Adding Visitors

The ExpansE web based application stores details for each visitor, associated card, and visitor access rights.

*To create visitors:*

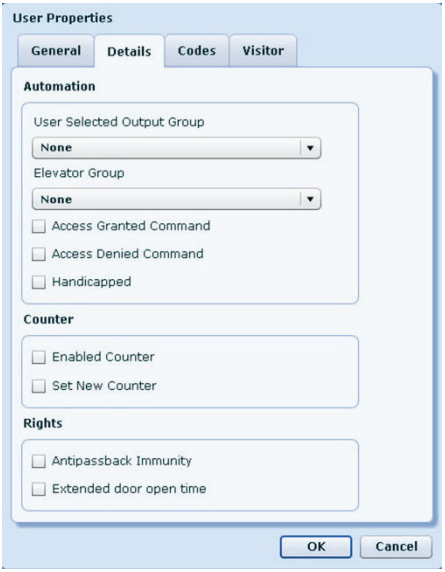
1. Expand the **Departments Visitors** element and select **Visitors**.
2. On the toolbar, click the icon.
   The *User Properties* window opens in the General tab.

**Figure 94: User Properties Visitor Window – General Tab**



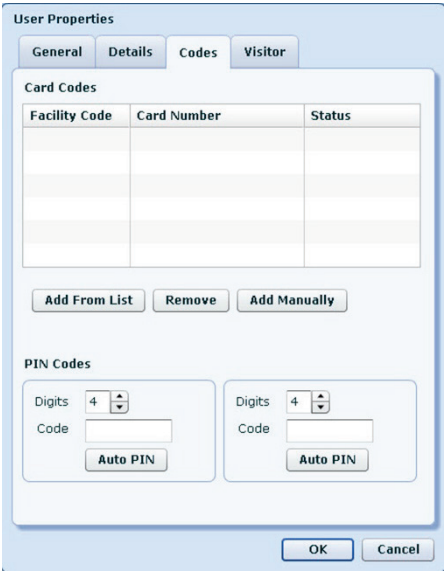

3. Enter the visitor's first name in the **First Name** field.
4. Enter the visitor's middle name in the **Middle Name** field.
5. Enter the visitor's last name in the **Last Name** field.
6. From the **Access Group** Select box, associate the visitor with an access group.
7. Set the access validity date and time. For limited access rights, select the **Until** checkbox and set the final date and time.
8. Click the *Details* tab to continue.

**Figure 95: User Properties Visitor Window – Details Tab**



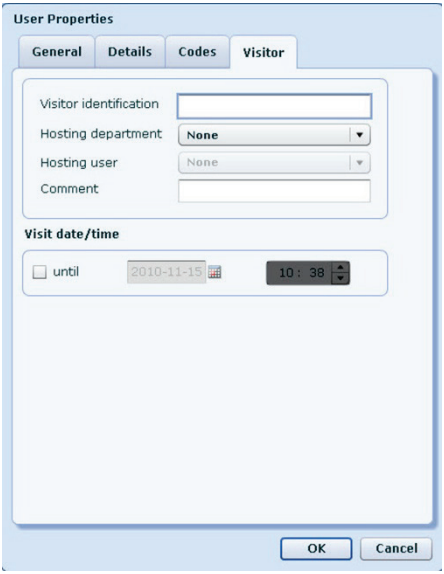

9. Set the Automation options:
   a. Select an output group previously created from the **User Selected Output Group** select box.
   b. Select an Elevator group previously created from the **Elevator Group** select box.
   c. Select the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
   d. Select the **Handicapped** checkbox to set handicapped privileges.
10. Set the counter options:
   a. Select the **Enable Counter** checkbox to activate the counter.
   b. Select the **Set New Counter** checkbox to reset the counter.
11. Set the access right options:
   a. Select the **Antipassback Immunity** checkbox to override any antipassback restrictions for this visitor.
   b. Select the **Extended door open time** checkbox to allow this user extended unlocked door duration. The extended duration is set for each door.
12. Click the *Codes* tab to continue.

**Figure 96: User Properties Visitor Window – Codes Tab**




13. Set the card associated to the visitor; you have one of several options to do so:
    a. Click the **Add From List** button to select a card already added to the system.
    b. Select a card from the list shown and click the **Remove** button to remove the card associated to the visitor.
    c. Click the **Add Manually** button to enter the card number then click the **Add From List** button to associate it with the visitor.
14. Define one or two PIN codes associated with the visitor:
    a. Define the length of the PIN for this visitor– enter a value or use the arrows in the **Digits** text box.
    b. Enter a PIN number based on the length defined in one or both of the **Code** text boxes.
    c. Click the **Auto PIN** button to automatically generate a random PIN.
15. Click the **Visitor** tab to continue.

**Figure 97: User Properties Visitor Window – Visitor Tab**




16. Enter an identification name for the user in the **Visitor identification** field.
17. Select the department hosting the user from the *Hosting department* list.
18. Add a host from the *Hosting user* list.
19. [Optional] Enter any additional comments in the Comment field.
20. Set the access validity for the visitor by setting the validity date and time.
21. Click **OK**.

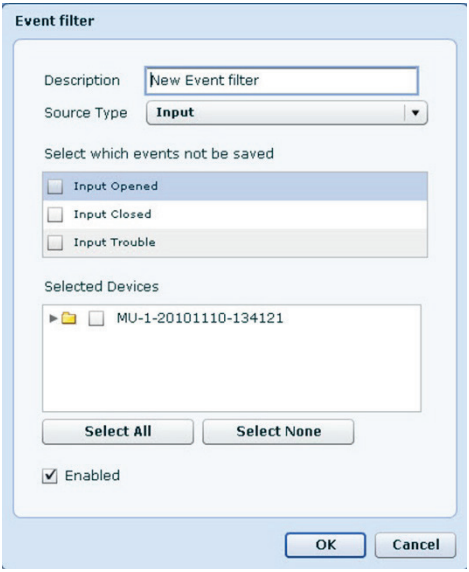
## 7.17 Setting Event Log Filters

You can set which events are viewed in the event log view and which are not.

*To set the event log filter:*

1. In the tree view, select the *Event Log Filter* option.
2. Click the icon.
   The *Event filter* window opens

**Figure 98: Even Filter Window**




3. In the **Description** field, enter a name for the event filter rule.
4. Select the devices associated with the event filter rule from the *Selected Devices* section. You can click **Select All** to add all of the devices or **Select None** to deselect all of the devices selected.
5. Select the source type from the **Source Type** list.
6. Select which events NOT to appear in the log file and not be saved in the system by selecting the checkbox next to each event.
7. Select the **Enabled** checkbox to activate the filter.
8. Click **OK**.

## 7.18 Defining Operators

Operators are people with access to the ExpansE web application. The default operator name is administrator.

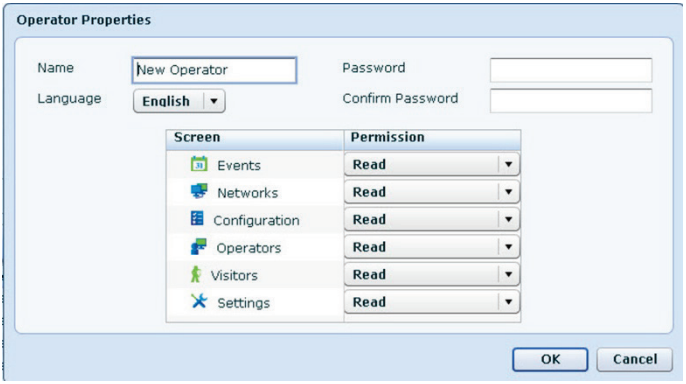
Different operators have wider or more restricted security rights, from complete control over the system to the ability only to view one section. All Operator passwords are case-sensitive.

*To define operators:*

1. In the tree view, select the *Operator* option.
2. Click the icon.

   The *Operator Properties* window opens.

**Figure 99: Operator Properties Window – New**




3. Enter the Operator's name in the **Name** Field.
4. Enter the operators' password in the **Password** field and re-enter the password in the **Confirm Password** field to confirm it.
5. Set the user interface language for this operator using the **Language** select box.
6. Set the operators permission rights for each of the screens.
7. Click **OK**.

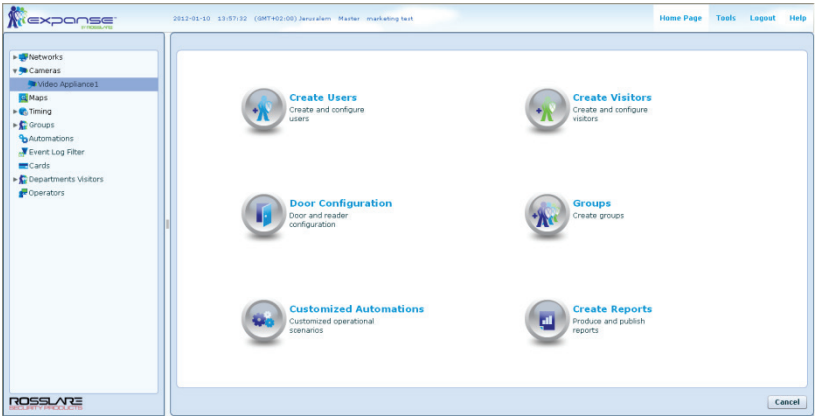
Note

Only one administrator can be logged in at one time.

# 8. Configuration Wizards

The ExpansE web-based application has several wizards for quick and simple configuration the wizards can be accessed at any time from the application's home page.

**Figure 100: ExpansE Wizards on Home Page**




## 8.1 Customized Automation Wizard

This wizard guides you in the process of associating various input and reader events with various output actions to create automated activities.

*To use the Automation Wizard:*

1. From the ExpansE homepage, click the **Customized Automations** icon.

**Figure 101: Customized Automation Wizard Icon**

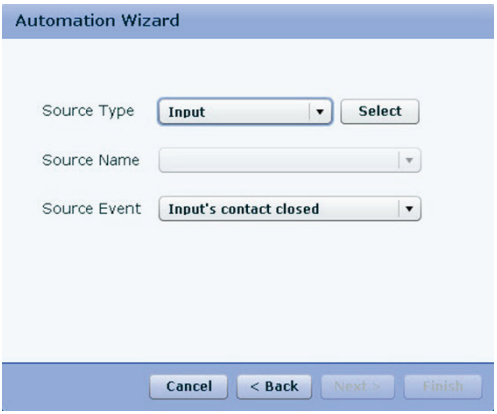
The customized automation welcome window opens.

**Figure 102: Customized Automation Wizard Welcome Page**

2. Enter a name for the process in the automation description field and click **Next**.

   The *Source Type* screen opens.

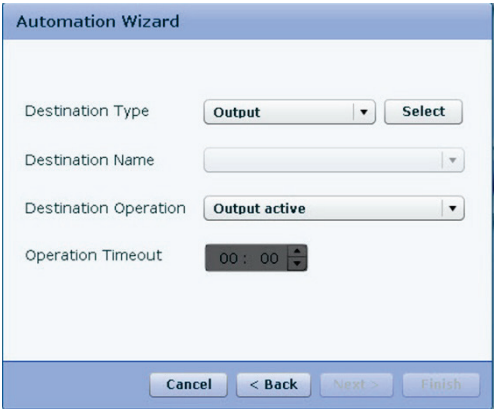
**Figure 103: Source Type Screen**




3. Pick the source type from the **Source Type** list and click **Select**.
4. Select the name of the source to use from the **Source Name** list, which appears after selecting a source type.
5. Select the event initiating the automated activity from the **Source Event** List.
6. Click **Next**.

   The *Destination Type* screen opens.

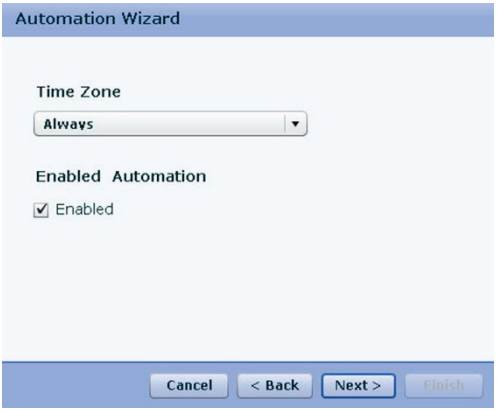
**Figure 104: Destination Type Screen**




7. Pick the destination type from the **Destination Type** list and click **Select**.
8. Select the name of the destination to use from the **Destination Name** list that appears after selecting a destination type.
9. Select the operation of the automated activity from the **Destination Operation** List.
10. Enter the minutes and seconds in the **Operation Timeout** field or use the up and down arrows to set the time frame for the operation timeout.
11. Click **Next**.

    The Automation screen opens.

**Figure 105: Automation Screen**



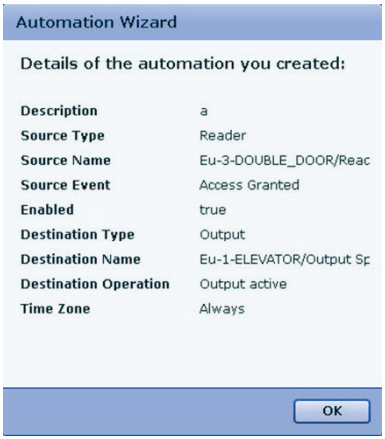

12. Select a time zone for this operation from the **Time Zone** list.
13. Select the **Enable** checkbox to enable the automated operation.
14. Click **Next** to complete the wizard process.

The Automation Wizard Complete window opens.

**Figure 106: Automation Wizard Complete Page**

15. Click **View Report** to open the automation report window.

**Figure 107: Automation Wizard – Report Window**




16. Click **OK** to close the window and return to the automation Wizard Complete page.
17. Click **Back** to go back and make changes if needed.
18. Click **Finish** to exit the wizard.

## 8.2 Create Users Wizard

The Create Users wizard guides you through the process of adding users, setting the user basic parameters, assigning a user to groups (if created, see Section 7.9), assigning user departments and other credentials.

*To use the user setup wizard:*

1. From the ExpansE homepage click the **Create Users** icon.

**Figure 108: Create User Wizard Icon**

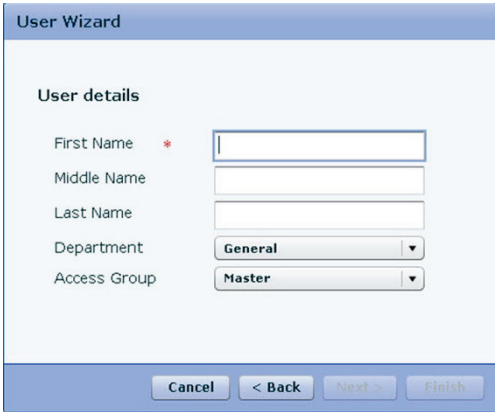
**Figure 109: User Wizard Welcome Page**

User Wizard
Welcome to create user wizard!!!
This wizard will guide you through the process of adding user, setting basic parameters, assigning to access groups, departments and credentials.
Cancel
< Back
Next >
Finish

2. The user wizard welcome window opens.
3. Click **Next** to move on to the next step.

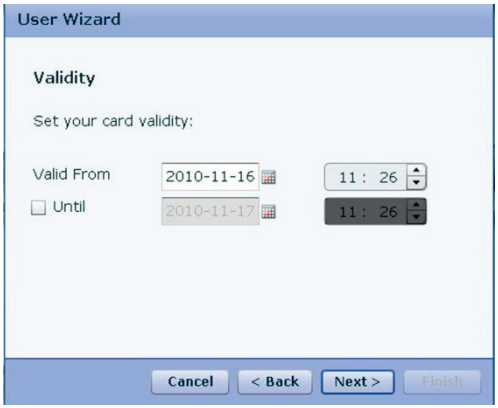
   The user details window opens.
4. Set the user details:
   a. Enter the user's first name in the **First Name** field; this field is mandatory.
   b. Enter the user's middle name in the **Middle Name** field if applicable.
   c. Enter the user's last name in the **Last Name** field.
   d. From the **Department** Select box, associate the user to one of the departments you created
   e. From the **Access Group** Select box, associate the user to one of the access groups you created

**Figure 110: User Wizard – User Details Page**



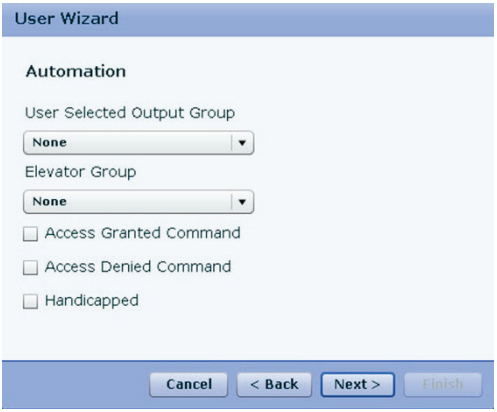

5. Click **Next** to move on to the next step.
   The Access Validity window opens.
6. Set the access validity date and time.
7. For limited access right, select the **Until** checkbox and set the final date and time.

**Figure 111: User Wizard – Validity Page**




8. Click **Next** to move on to the next step.
   The Automation window opens.

**Figure 112: User Wizard – Automation Page**




9. Set the Automation options:
   a. Select an output group previously created from the **User Selected Output Group** select box.
   b. Select an Elevator group previously created from the **Elevator Group** select box.
   c. Select the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
   d. Select the **Handicapped** checkbox, to set handicapped privileges.
10. Click **Next** to move on to the next step.

    The Access rights window opens.

**Figure 113: User Wizard – Access Rights Page**

11. Set the counter options:
    a. Select the **Enable Counter** checkbox, to activate the counter.
    b. Select the **Set New Counter** checkbox, to reset the counter.
12. Set the access right options:
    a. Select the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this user.
    b. Select the **Extended door open time** checkbox, to allow this user extended unlocked door duration. The extended duration is set for each door.
13. Click **Next** to move on to the next step.

    The card association window opens.

**Figure 114: User Wizard – Card Association Page**

14. Set the card associated to the user, you have one of several options to do so:
    a. Click the **Add From List** button to select a card already added to the system.
    b. Select a card from the list shown and click the **Remove** button to remove the card associated to the user.
    c. Click the **Add Manually** button to enter the card number and associate it with the user.
15. Click **Next** to move on to the next step.

    The PIN code association window opens.

**Figure 115: User Wizard – PIN Code Association Page**

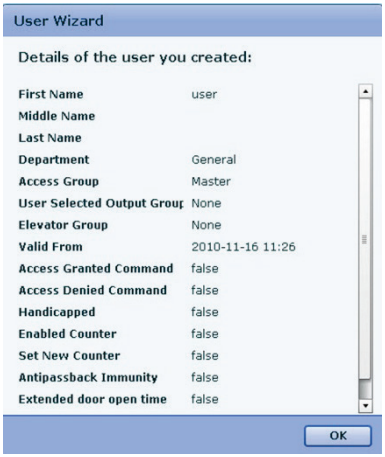
16. Define one or two PIN codes associated with the user:
    a. Define the length of the PIN for this user, enter a value or use the arrows in the **Digits** textbox.
    b. Enter a PIN number based on the length defined in one or both of the **Code** text boxes.
    c. Click the **Auto PIN** button to automatically generate a random PIN code.
17. Click **Next** to complete the wizard process.

    The User Wizard Complete window opens.

**Figure 116: User Wizard Complete Page**

18. Click **View Report** to open the user report window.

**Figure 117: User Wizard – User Report Window**




19. Click **OK** to close the window and return to the User Wizard Complete page.
20. Click **Add new user** to return to step 3 and repeat the process for an additional user. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

## 8.3 Create Visitors Wizard

The Create Visitor wizard guides you through the process of adding users that are defined as visitors.

*To use the visitor setup wizard:*

1. From the ExpansE homepage click the **Create Visitors** icon.

**Figure 118: Create Visitor Wizard Icon**

The Visitor wizard welcome window opens.

2. Click **Next** to move on to the next step. The user details window opens.

**Figure 119: Visitor Wizard Welcome Page**

Visitor Wizard
Welcome to create visitor wizard
This wizard will guide you through the process of adding visitor, setting basic parameters, assigning to access groups, departments and credentials
Cancel
< Back
Next >
Finish

3. Set the user details:
   a. Enter the user's first name in the **First Name** field; this field is mandatory.
   b. Enter the user's middle name in the **Middle Name** field if applicable.
   c. Enter the user's last name in the **Last Name** field.
   d. From the **Access Group** Select box, associate the user to one of the access groups you created

**Figure 120: Visitor Wizard – Visitor's Details Page**

4. Click **Next** to move on to the next step.
   The Access Validity window opens.
5. Set the access validity date and time.
6. Select the **Until** checkbox and set the final date and time for the visitor's access rights.

**Figure 121: Visitor Wizard – Validity Page**

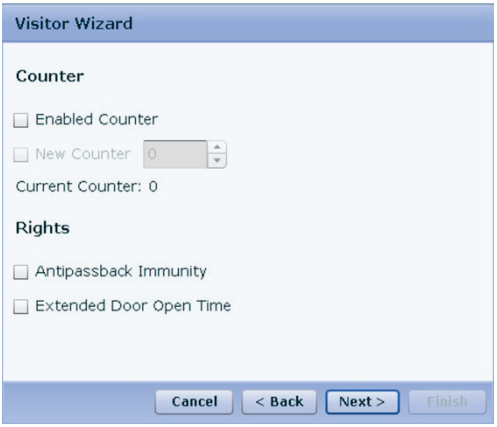
7. Click **Next** to move on to the next step, the Automation window opens.

**Figure 122: Visitor Wizard – Automation Page**

8. Set the Automation options:
   a. Select an output group previously created from the **Output Group** select box.
   b. Select an Elevator group previously created from the **Elevator Group** select box.
   c. Select the **Access Granted Command** or **Access Denied Command** checkboxes to set the command activation method.
   d. Select the **Handicapped** checkbox, to set handicapped privileges.
9. Click **Next** to move on to the next step.

   The Access rights window opens.

**Figure 123: Visitor Wizard – Access Rights Page**




10. Set the counter options:
    a. Select the **Enable Counter** checkbox, to activate the counter.
    b. Select the **Set New Counter** checkbox, to reset the counter.
11. Set the access right options:
    a. Select the **Antipassback Immunity** checkbox, to override any antipassback restrictions for this visitor.
    b. Select the **Extended door open time** checkbox, to allow this visitor extended unlocked door duration. The extended duration is set for each door.
12. Click **Next** to move on to the next step.

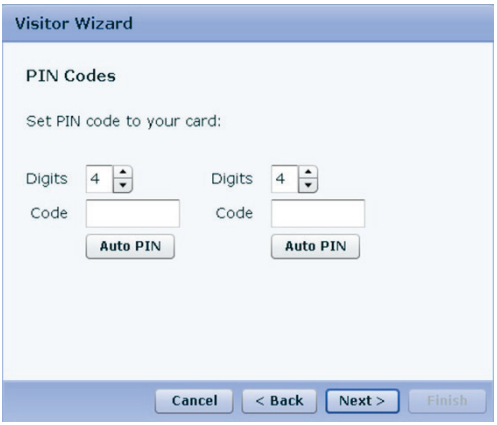
    The card association window opens.

**Figure 124: Visitor Wizard – Card Association Page**

13. Set the card associated to the visitor, you have one of several options to do so:
    a. Click the **Add From List** button to select a card already added to the system.
    b. Select a card from the list shown and click the **Remove** button to remove the card associated to the visitor.
    c. Click the **Add Manually** button to enter the card number and associate it with the visitor.
14. Click **Next** to move on to the next step.

    The PIN code association window opens.

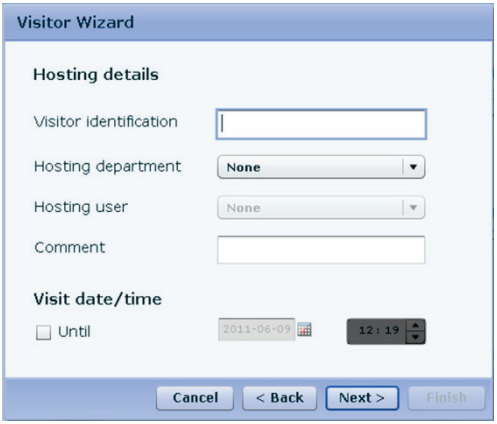
**Figure 125: Visitor Wizard – PIN code association Page**




15. Define one or two PIN codes associated with the visitor:
    a. Define the length of the PIN for this visitor– enter a value or use the arrows in the **Digits** text box.
    b. Enter a PIN number based on the length defined in one or both of the **Code** text boxes.
    c. Click the **Auto PIN** button to automatically generate a random PIN code.
16. Click **Next** to move on to the next step.

    The host association window opens.

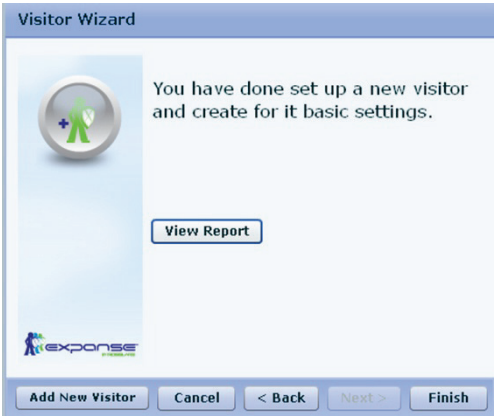
**Figure 126: Visitor Wizard – Host Association Page**




17. Define the visitor's host details:
    a. Enter identification, such as a company name, for the visitor in the **Visitor identification** text box.
    b. Select the department hosting the visitor from the **Hosting department** select box.
    c. Select the user within the selected department hosting the visitor from the **Hosting user** select box.
    d. Enter comments if applicable in the **Comment** text box.
    e. Select the **Until** checkbox and set the date and time for the conclusion of the scheduled visit.
18. Click **Next** to complete the wizard process.

    The Visitor Wizard Complete window opens.

**Figure 127: Visitor Wizard Complete Page**




19. Click **View Report** to open the Visitor report window.

20. Click **OK** to close the window and return to the Visitor Wizard Complete page.
21. Click **Add New Visitor** to return to step 3 and repeat the process for an additional visitor. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

## 8.4 Doors Wizard

The doors wizard guides you through the process of adding doors to the system and configuring them.

*To use the Doors wizard:*

1. From the ExpansE homepage click the **Door Configuration** icon.

**Figure 128: Doors Wizard Icon**

The *Door Wizard* welcome window opens.

2. Click **Next** to move on to the next step.

   The door selection window opens.

**Figure 129: Doors Wizard – Welcome Page**

Door Wizard
Welcome to door configuration wizard
This Wizard will guide you through the process of adding a door, setting basic parameters, configuring readers and door behavior.
Cancel
< Back
Next >
Finish

3. Select the door EU you wish to define from the list of EUs under each MU.

**Figure 130: Doors Wizard – Door Selection Page**

4. Click **Next** to move on to the next step.

   The Door Details window opens.

**Figure 131: Doors Wizard – Door Details Page**

5. Define the door details:
   a. Enter a description for the selected door in the **Description** text box.
   b. Determine the door polarity by selecting or clearing the **Door output polarity is Normally Closed** checkbox.

      Select this checkbox to ensure Fail Safe door opening if the Fail Safe door Lock Device power fails.

      Once enabled, the door output relay is activated when the door is closed, and is deactivated when the door is open.

      In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals

c. Select the **REX enabled** checkbox to allow Requests to Exit for this door.
d. Select the **Manual Door Open Enabled** checkbox to allow operators to adjust the door manually. See Section 9.1.
e. Select the **Timezone Logic** checkbox to initiate the time zone logic options and select the desired output from the list.
f. Select the **First person Delay** checkbox to keep the door locked until the first user opens it.

6. Click **Next** to move on to the next step.

   The Door Timers window opens.

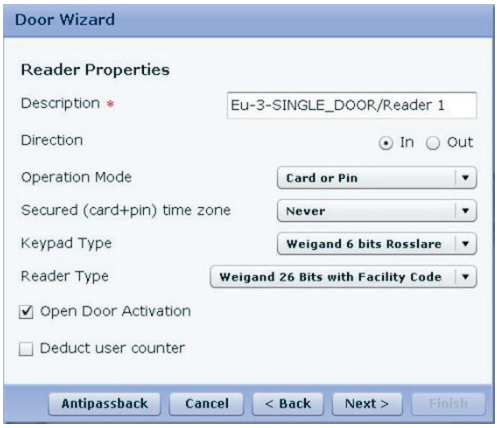
**Figure 132: Doors Wizard – Door Timers Page**

7. Define the various timers for the doors:
   a. Set the duration for which the door stays unlocked by typing minutes and seconds in the **Door open time** field or use the associated up and down arrows.
   b. Set the duration for which the door stays unlocked for users with Extended door open rights by typing minutes and seconds in the **Extended Door open time** field or use the associated up and down arrows.
   c. Set the duration following which and when the door is forced open, an event occurs.
   d. Select the **Door forced** checkbox to use this timer.
   e. Enter the minutes and seconds in the associated field or use the up and down arrows.
   f. Set the duration for which the door can be held open without raising an alarm event.
   g. Select the **Door held open** checkbox to use this timer and enter the minutes and seconds in the associated field or use the up/down arrows.

8. Click **Next** to move on to the next step.

   The Reader Properties window opens.

**Figure 133: Doors Wizard – Reader Properties Page**




9. Define the reader properties associated with the door:
   a. In the **Description** field, enter a name for the reader.
   b. Select whether the reader is allowing entry into the area or exit out of the area by selecting either the **In** or **Out** option.
   c. From the Operation Mode list Select how the reader operates:
      i. **Inactive:** The reader is not in use.
      iii. **Card Only:** The reader accepts RFID cards only.
      iv. **PIN Only:** The reader accepts PIN inputs only.
      v. **Card or PIN:** The reader accepts both cards and PIN codes.
      vi. **Desktop:** The reader is inactive, but is being used to record new cards on the computer.
      vii. **No Access Mode:** The reader grants access to no users.
   d. Using the **Secured (Card+PIN) time zone** list select a time zone during which access should be granted only after both the card and PIN are entered.

      The PIN must be entered within 10 seconds of card entry.
   e. From the **Keypad Type** list, select the data transmission type for the type of keypad hardware.
   f. From the **Reader Type** list, select the data transmission type for the reader hardware.
   g. Select the **Open Door Activation** checkbox to allow the reader to unlock the door.
   h. Select the **Deduct User Counter** checkbox to record this entry against the user's entry allowance counter.
10. Click **Next** to complete the wizard process.

The Door Wizard Complete window opens.

**Figure 134: Door Wizard – Complete Page**

11. Click **View Report** to open the door report window.

**Figure 135: Door Wizard – Report Window**

12. Click **OK** to close the window and return to the Door Wizard Complete page.
13. Click **Back** to go back and make changes if needed.
14. Click **Finish** to exit the wizard.

## 8.5 Groups Wizard

The Groups wizard guides you through the process of creating the various available groups in the system: Access groups, Input Groups, Output Groups, and Elevator groups.

### 8.5.1 Access Groups

This section describes the use of the Groups wizard when creating Access Groups.

*To create access groups using the Groups wizard:*

1. From the ExpansE homepage click the **Groups** icon.

**Figure 136: Groups Wizard Icon**

The Groups wizard welcome window opens.

2. Choose Access Groups from the **Select Group** select box.

**Figure 137: Groups Wizard Welcome Page**

3. Click **Next** to move on to the next step.

The Access group definition window opens.

**Figure 138: Groups Wizard – Access Group Definition Page**

4. In the **Description** field, enter a name for the access group.
5. From the *Readers List* select the readers you wish to associate with this group and click **Add**.
6. For each of the readers select a time zone association.
7. Select a reader and then click **Remove** to remove the readers from the association list.
8. Click **Next** to complete the wizard process.

   The Groups Wizard Complete window opens.

**Figure 139: Groups Wizard Complete Page**

9. Click **Back** to go back and make changes if needed. Click **Finish** to exit the wizard.

### 8.5.2 Input Groups

This section describes the use of the Groups wizard when creating Input Groups.

*To create input groups using the Groups wizard:*

1. From the ExpansE homepage click the **Groups** icon.

**Figure 140: Groups Wizard Icon**

The Groups wizard welcome window opens.

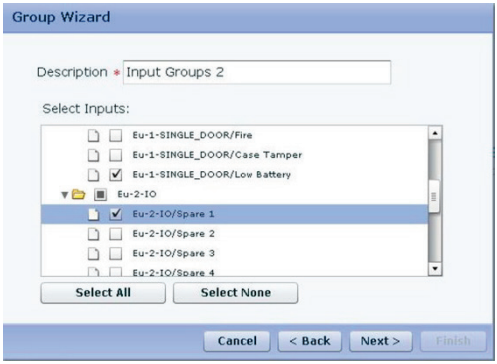
2. Choose Input Groups from the **Select Group** select box.

**Figure 141: Groups Wizard Welcome Page**

3. Click **Next** to move on to the next step.

The Input group definition window opens.

**Figure 142: Groups Wizard – Input Group Definition Page**




4. In the **Description** field, enter a name for the input group.
5. Within *Select inputs*, select all the inputs you wish to add.
6. Click **Select All** to add all of the inputs shown.
7. Click **Select None** to deselect all of the inputs selected.
8. Click **Next** to complete the wizard process.
   The Groups Wizard Complete window opens.

**Figure 143: Groups Wizard Complete Page**

9. Click **Back** to go back and make changes if needed.
10. Click **Finish** to exit the wizard.

### 8.5.3 Output Groups

This section describes the use of the Groups wizard when creating Output Groups.

*To create output groups using the Groups wizard:*

1. From the ExpansE homepage click the **Groups** icon.

**Figure 144: Groups Wizard Icon**

The Groups wizard welcome window opens.

2. Choose Output Groups from the **Select Group** select box.

**Figure 145: Groups Wizard Welcome Page**

3. Click **Next** to move on to the next step.

The Output group definition window opens.

**Figure 146: Groups Wizard – Output Group Definition Page**

4. In the **Description** field, enter a name for the output group.
5. Within *Select outputs*, select all the inputs you wish to add.
6. Click **Select All** to add all of the output shown.
7. Click **Select None** to deselect all of the outputs selected.
8. Click **Next** to complete the wizard process.
   The Groups Wizard Complete window opens.

**Figure 147: Groups Wizard Complete Page**

9. Click **Back** to go back and make changes if needed.
10. Click **Finish** to exit the wizard.

### 8.5.4 Elevators Groups

This section describes the use of the Groups wizard when creating Elevators Groups.

*To create elevators groups using the Groups wizard:*

1. From the ExpansE homepage click the **Groups** icon.

**Figure 148: Groups Wizard Icon**

The Groups wizard welcome window opens.

2. Choose Elevators Groups from the **Select Group** select box.

**Figure 149: Groups Wizard Welcome Page**

3. Click **Next** to move on to the next step.

The Elevators group definition window opens.

**Figure 150: Groups Wizard – Output Group Definition Page**

4. In the **Description** field, enter a name for the elevator group.
5. Within *Reader List* select and click **Add** for all the readers you wish to add to the group.
6. For each reader:
   a. Select a time zone association from the **Timezone** select box.
   b. Select the associated output group from the **Output Group** select box.
7. Select a reader and then click **Remove** to remove the readers from the association list.
8. Click **Next** to complete the wizard process.

   The Groups Wizard Complete window opens.

**Figure 151: Groups Wizard Complete Page**

9. Click **Back** to go back and make changes if needed.
10. Click **Finish** to exit the wizard.

# 9. Manual Operation

In addition to automated monitoring and control of the access control network, it is also possible to control certain functionality in the network directly from the ExpansE web based application.

Note

Door Manual Operation can only control doors that have **Manual Door Open Enabled** selected in the *Door Properties* window.

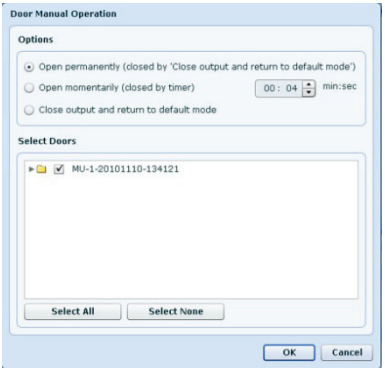
## 9.1 Manual Door Control

The *Door Manual Operation* window allows an operator to open or close a selected group of doors directly.

*To manually open or close a door:*

1. On the toolbar, click the **Open Door Manually** icon.
   The *Door Manual Operation* window opens.

**Figure 152: Door Manual Operation Window**




2. Select an option:
   - **Open permanently** – All selected doors are opened.
   - **Open momentarily** – All selected doors are opened for the time set in the timer box.
   - **Close output** – Close the selected doors and return to default mode.
3. Select the checkboxes of those doors to which to apply the operation.
4. Click **OK**.

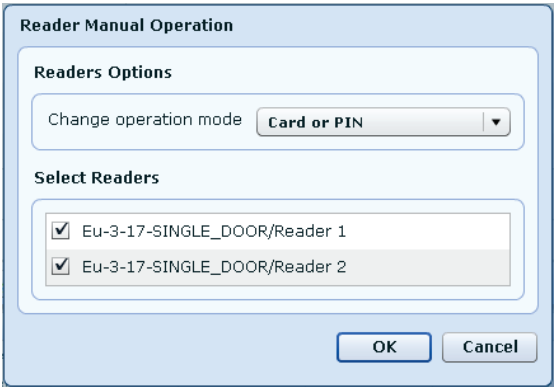
## 9.2 Manual Reader Control

The *Manual Reader Operation* window allows an operator to manually change the operation mode of a reader.

*To manually change the operation mode of a reader:*

1. In the tree view, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.
3. Click **Readers**.
4. On the toolbar, click the **Reader Manual Operation** icon.
   The *Reader Manual Operation* window opens.

**Figure 153: Door Manual Operation Window**




5. In **Change operation mode**, select the desired operation mode.
6. Select the checkboxes of those doors to which to apply the operation mode.
7. Click **OK**.

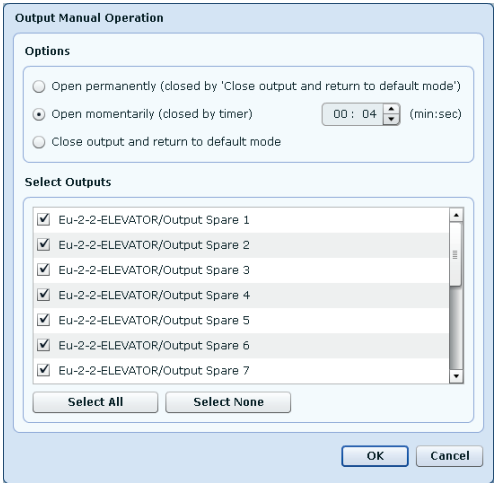
## 9.3 Manual Output Control

The *Manual Output Operation* window allows an operator to manually open or close an output.

*To manually open or close an output:*

1. In the tree view, click **Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the tree view.
3. Click **Outputs**.
4. On the toolbar, click the **Output Manual Operation** icon.
   The *Output Manual Operation* window opens.

**Figure 154: Door Manual Operation Window**




5. Select an option:
   - **Open permanently** – All selected outputs are opened.
   - **Open momentarily** – All selected outputs are opened for the time set in the timer box.
   - **Close output** – Close the selected outputs and return to default mode.
6. Select the checkboxes of those outputs to which to apply the operation.
7. Click **OK**.

# 10. ExClouds

ExClouds is a module that offers two additional features to the ExClouds application

ExClouds Application – To generate reports from the ExClouds database

ExClouds Web Server – To generate reports from the ExClouds database and to access surveillance cameras that are connected to your security network

## 10.1 ExClouds Application

The ExClouds application allows generating various reports using the data stored in system database. This section refers to the ExClouds software required for generating reports.

### 10.1.1 Minimum Requirements

- Supported Operating Systems:
  - Windows XP SP3
  - Windows Server 2003 SP2
  - Windows Vista SP1 or later
  - Windows Server 2008 (not supported on Server Core Role)
  - Windows 7
  - Windows Server 2008 R2 (not supported on Server Core Role)
- Supported Architectures:
  - x86
  - x64
  - ia64 (some features are not supported on ia64 for example, WPF)
- Hardware Requirements:
  - Recommended Minimum: Pentium 1 GHz or higher with 512 MB RAM or more
  - Minimum disk space:
    - x86 – 850 MB
    - x64 – 2 GB

### 10.1.2 ExClouds Application Installation

The ExClouds installation consists of two steps:

- Installing the ExClouds Software
- Installing the Report Module

#### 10.1.2.1 Installing the ExClouds Software

*To install the ExClouds application software:*

1. Double-click on the ExClouds Setup.exe file in the CD provided or in the folder where you saved the installation package you received from Rosslare.

   The Welcome screen opens.

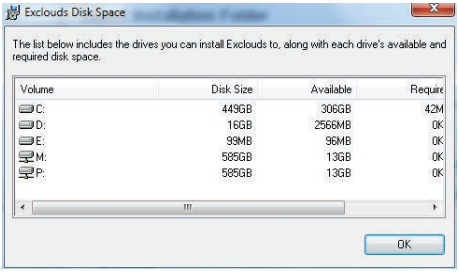
2. Click **Next**.

   The *Select Installation Folder* window opens.

3. Enter the installation location in the **Folder** field. Alternatively use the **Browse...** button to select an installation location.

4. Use the **Disk Cost...** button to show available space on your computer.

**Figure 155: ExClouds – Disk Space Screen**




5. Select the availability of the software to users using the computer between **Everyone** or **Just me**, and click **Next** to continue.

   The *Confirm Installation* window opens.

6. Click **Next** to confirm the installation and to initiate the installation process.

   The *Installing ExClouds* window opens.

   Once the progress bar indicates that the installation process is complete, the *Installation Complete* window opens.

7. Click **Close** to exit the installation setup.

#### 10.1.2.2 Installing the Report Module

*To install the Report Module:*

1. Locate the CRRedist2008_x86.msi file in the same location as the setup file.

2. Double-click the file to begin the installation process.

   Once complete, the installation window closes automatically.

### 10.1.3 ExClouds Setup

Once the ExClouds software is installed, you must configure it to work with the ExpansE web application.

*To configure the ExClouds software:*

1. Click the ExClouds icon from either the desktop or the start menu.
   The ExClouds software login screen opens.

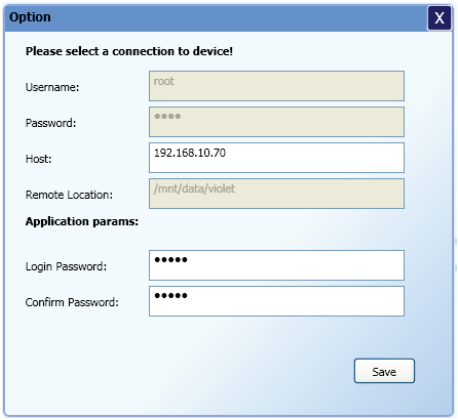
**Figure 156: ExClouds – Login Screen**

2. Enter your password and click **Login**. The default password is *admin*.
   The ExClouds main window opens

**Figure 157: ExClouds – Main Window**

3. Click the **Settings** icon.
   The *Option* window opens.

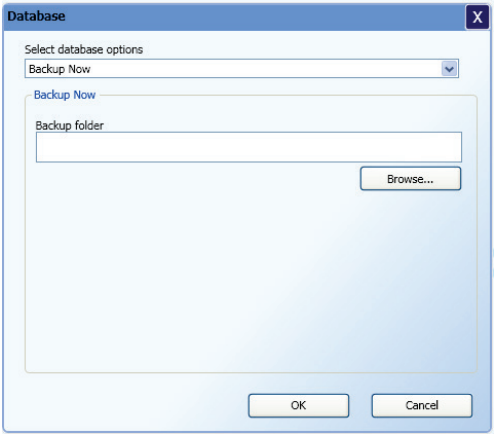
**Figure 158: ExClouds – Option Window**




4. Define the Host ExpansE system by entering the ExpansE's IP in address In the **Host** field.
5. Enter the ExpansE's user name in the **Username** field.
6. Enter ExpansE's password corresponding with the user name entered in the **Password** field.
7. Define the ExClouds password in the **Login Password** and **Confirm Password** fields and click **Save**.
8. Click the **Database** icon.

   The *Database Option* window opens.

**Figure 159: ExClouds – Database Option Window**




9. Choose between uploading the database and backing up the existing database if the system is already configured and running.

You can initiate the various reports directly from the ExClouds software by selecting the desired report from the tree view on the left. See the various report options and complete instruction on each report in Chapter 11.

### 10.1.4 Tools Menu

When the ExClouds application is installed, two additional options are available in the Tools menu:

- Database Actions
- Create Reports

#### 10.1.4.1 Database Actions

Database Actions allows you to either back up the database or restore the database from a previously-saved file.

#### 10.1.4.2 Creating Reports

Clicking Create Reports on the Home page opens the Report Wizard, which is also available on the Home Page. Details on how to generate various reports are described in Chapter 11.

## 10.2 ExClouds Web Server

In addition to allowing you to generate reports as with the ExClouds application, the ExClouds web server allows you access surveillance cameras that are connected to your security system. The web server allows you to view and configure camera streams in real-time, as well as to record and download them.

The ExClouds application allows generating various reports using the data stored in system database. This section refers to the ExClouds software required for generating reports.

### 10.2.1 Minimum Requirements

- Supported Operating Systems:
  - Windows XP SP3
  - Windows Server 2003 SP2
  - Windows Vista SP1 or later
  - Windows Server 2008 (not supported on Server Core Role)
  - Windows 7
  - Windows Server 2008 R2 (not supported on Server Core Role)
- Supported Architectures:
  - x86
  - x64
  - ia64 (some features are not supported on ia64 for example, WPF)

- Hardware Requirements:
  - Minimum RAM: 2 GB
  - Minimum disk space: 50 GB

### 10.2.2 Software Prerequisite

Before you can install the ExClouds Web Server software, you must install the VMware Player application.

*To install VMware Player:*

1. Download the application from the Internet, which can be found at: http://www.vmware.com/products/player
2. Double-click the Setup file.
3. A standard Security Warning window opens.
4. Click **Run**.
5. The *VMware Player Setup* window opens.

   After a few moments, this window closes and the VMware Player welcome screen opens.
6. Click **Next**.

   The Destination Folder screen opens.
7. Click **Next** through the next three screens.
8. The Ready to Perform the Requested Operations screen opens.
9. Click **Continue**.
10. The Performing the Requested Operations screen opens.

    After a few moments, this window closes and the *Setup Wizard Complete* screen opens.
11. Click **Restart Now** to restart your PC and finish the installation.

### 10.2.3 ExClouds Web Server Installation

*To install the ExClouds Web Server software:*

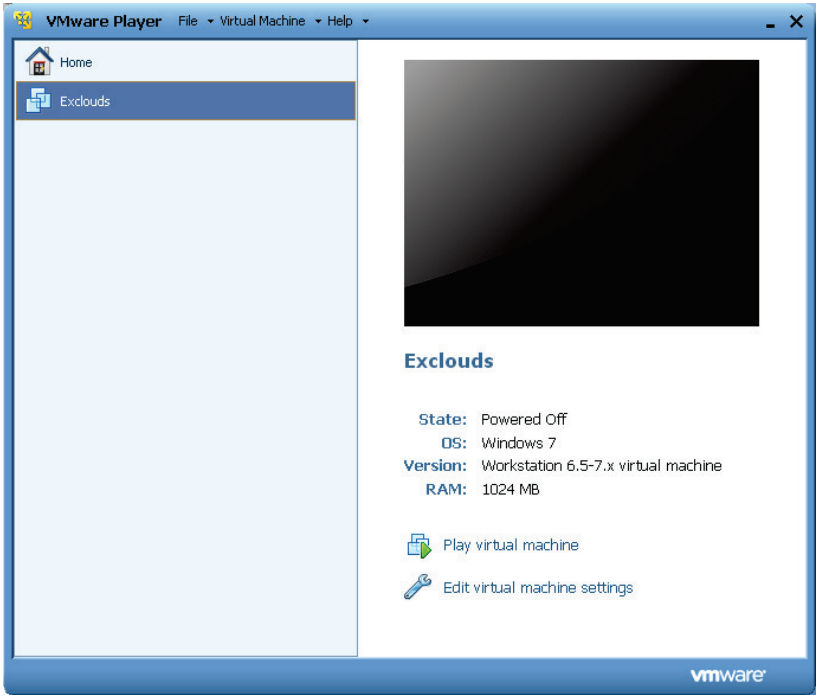
1. Unzip the contents of the ExClouds.zip file found on the CD provided to your local PC.
2. Open the VMware Player application.

**Figure 160: VMware Player Window**

VMware Player
File
Virtual Machine
Help
Home
Welcome to VMware Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation
Get advanced features such as snapshots, record/replay, teams, developer tool integration, and more.
Help
View VMware Player's help contents.
vmware

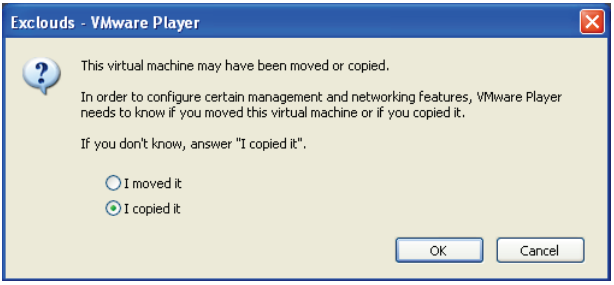
3. Click **Open a Virtual Machine**.
   A standard browse dialog opens.
4. Locate and select the Exclouds.vmx file.
5. The ExClouds icon appears on in the left pane.

**Figure 161: ExClouds icon in VMware Player Window**



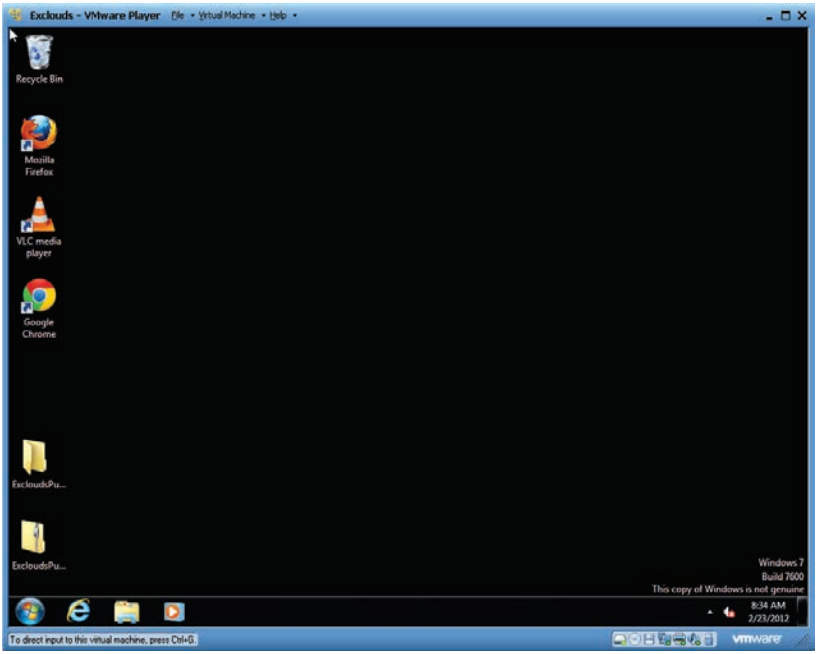

6. Double-click the ExClouds icon in the VMware Player window.
   The following window opens:

**Figure 162: ExClouds – WMware Player Window**


Excloud - VMware Player
This virtual machine may have been moved or copied.
In order to configure certain management and networking features, VMware Player needs to know if you moved this virtual machine or if you copied it.
If you don't know, answer "I copied it".
I moved it
I copied it
OK
Cancel

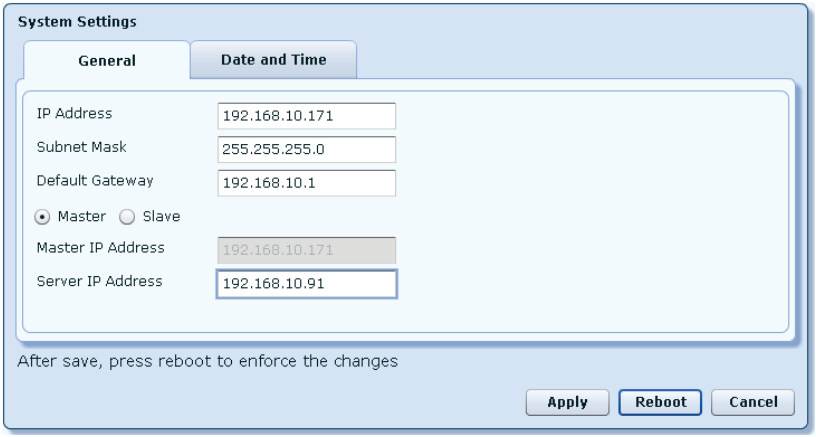
7. Choose **I copied it** and click **OK**.
   A virtual Windows session opens in a new window.

**Figure 163: ExClouds Virtual Machine Window**




8. In the virtual window, set the IP address as described in Section 6.1 and remember it.
9. On your local PC, open the ExpansE application.
10. Click **Tools>Settings**.
11. In the **Server IP address** field, enter the IP address that you set in Step 8.

**Figure 164: Setting Server IP Address**




12. Click **Apply** and then **Reboot**.

    Wait two minutes until the new settings in the ExpansE application are applied.

13. To enter ExpansE using the ExClouds Web Server, enter the following in your web browser:

    **ExClouds Server IP address/IP of MU**

    For example: 192.168.10.91/192.168.10.171

Note

The VMware window must remain open at all times during the ExClouds Web Server session.

### 10.2.4 Viewing the Camera Stream

*To view connected cameras:*

1. In the Tree View, click **Cameras**.

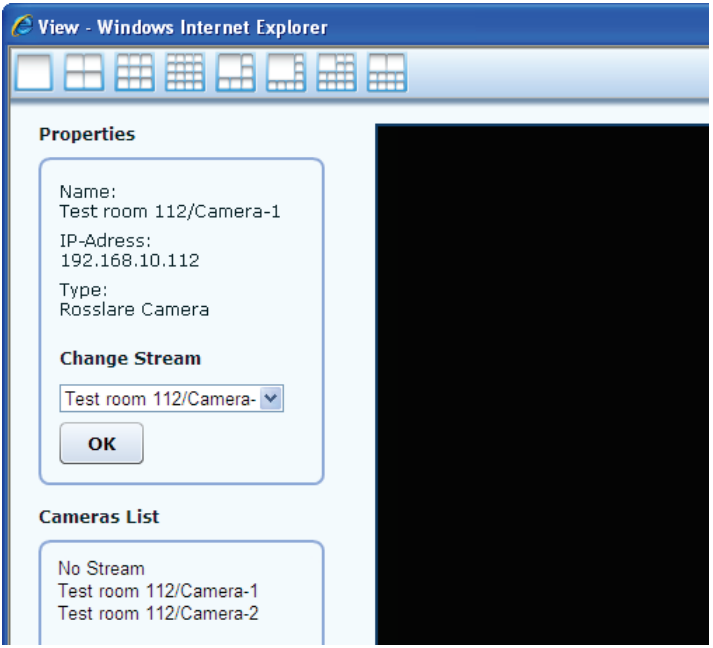
   The available cameras are listed in the display area.

2. Select a camera from the list.

3. Click the icon.

   A new browser window opens showing a stream of the first listed camera.

**Figure 165: Live Camera Stream**




4. If you wish to change the stream you are viewing:
   a. Click the **Change Streams** checkbox.
   b. Choose the stream you wish to view.
   c. Click **OK**.
5. To change the view of the stream, click the various buttons at the top of the page (Figure 165).

**Figure 166: Buttons to Change Stream View**

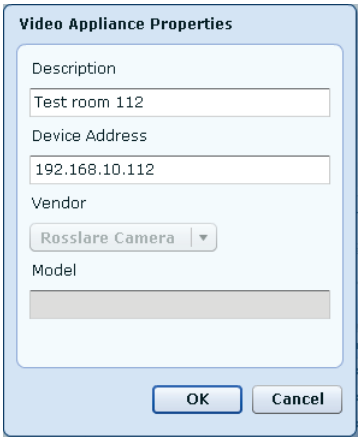
### 10.2.5 Editing Camera Properties

*To edit the properties of a camera:*

1. In the Tree View, click **Cameras**.
   The available cameras are listed in the display area.
2. Select a camera from the list.
3. Click the icon.

The Video Appliance Properties window opens.

**Figure 167: Video Appliance Properties Window**




4. Change the Description and the Device Address of each camera as needed.
5. Click **OK**.

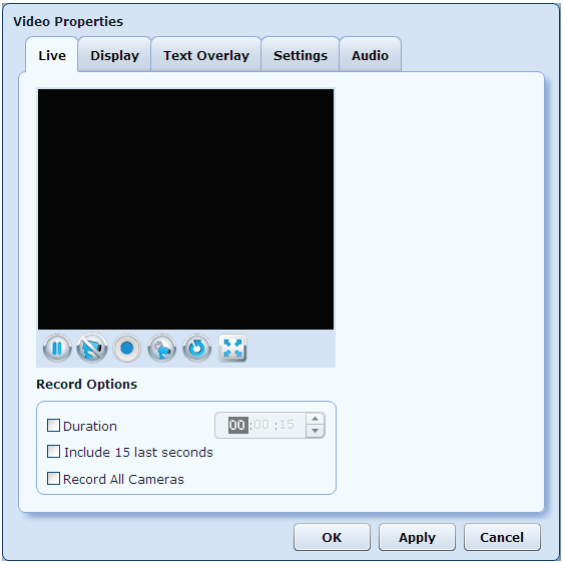
### 10.2.6 Recording and Configuring Camera Streams

Recording and configuring camera streams is performed using the *Video Properties* window, which consists of five tabs.

#### 10.2.6.1 Live Tab

The *Live* tab (Figure 167) is used to manually record a live stream using various buttons and checkboxes that appear below the stream.

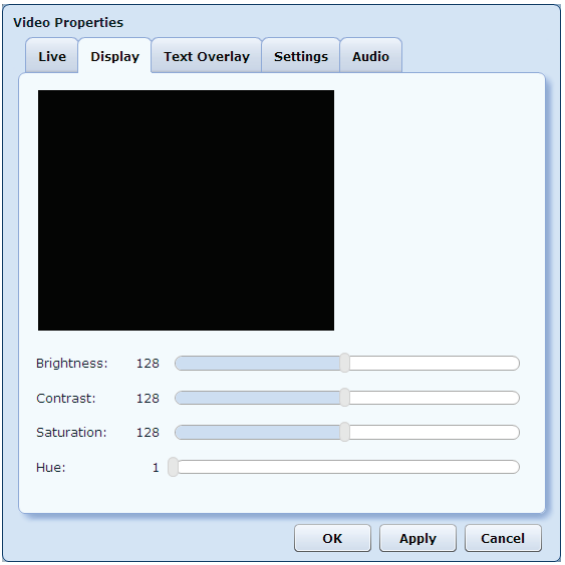
**Figure 168: Video Properties – Live Tab**




### 10.2.6.2 Display Tab

Use the *Display* tab (Figure 168) to adjust the various properties of the stream appearance.

**Figure 169: Video Properties – Display Tab**

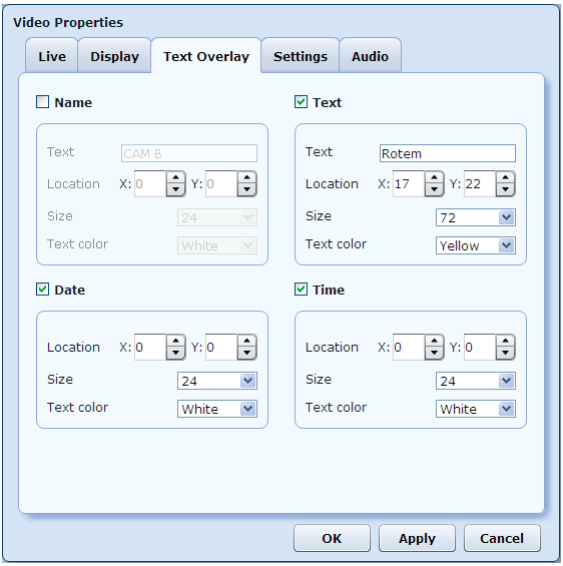


### 10.2.6.3 Text Overlay Tab

The *Text Overlay* tab allows you to add text to appear on the stream. You can choose between four fields: Name, Text, Date, and Time.

For each field, you can choose the location, size, and color of the text that appears.

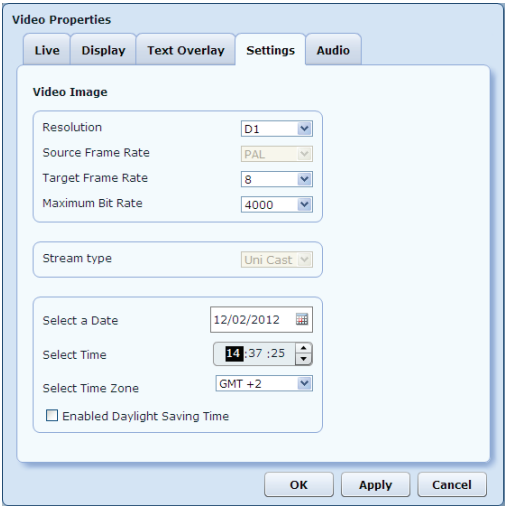
**Figure 170: Video Properties – Text Overlay Tab**



### 10.2.6.4 Settings Tab

With the *Settings* tab, you can adjust the characteristics of the stream itself, such as the resolution and bit rate. In addition, you can set the date, time, and time zone of the stream.

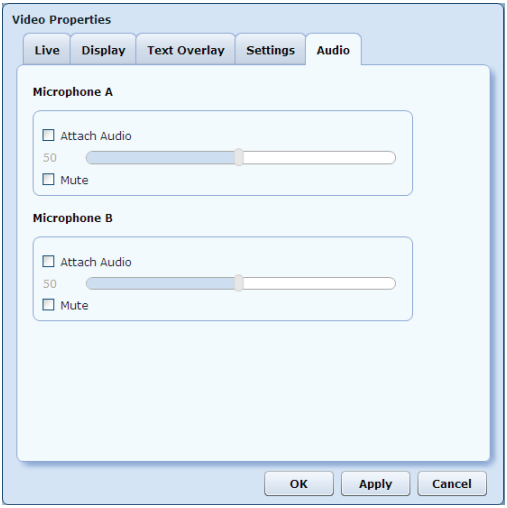
**Figure 171: Video Properties – Settings Tab**




### 10.2.6.5 Audio Tab

The audio tab allows you to add audio to the captured camera stream.

**Figure 172: Video Properties – Audio Tab**



*To record and configure camera streams:*

1. In the Tree View, click **Cameras** and expand the tree view.
2. In the Tree View, select a camera from the list.
3. The cameras connected to this camera EU are listed in the display area.
4. Double-click on a camera from the list.
   The *Video Properties* window opens.
5. Use the five tabs described above to record video or configure the streaming properties.

### 10.2.7 Downloading Camera Streams

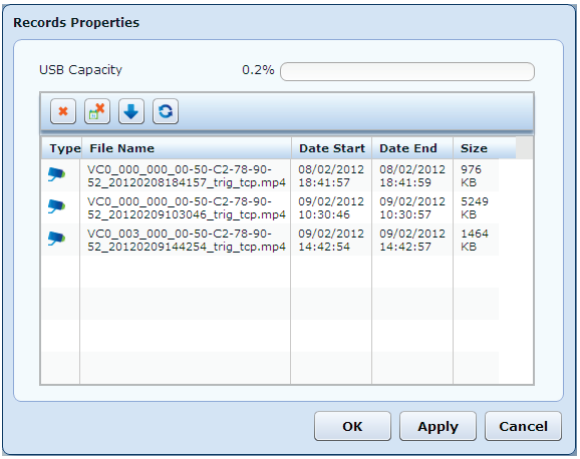
Any stream that has been recorded is saved on the connected USB stick.

These streams can then be downloaded to your PC.

*To download a camera stream:*

1. In the Tree View, click **Cameras**.
   The available cameras are listed in the display area.
2. Select a camera from the list.
3. Click the icon.
4. The *Records Properties* window opens.

**Figure 173: Records Properties Window**




5. Select a clip to download.
6. Click the icon.
7. A standard Windows File Download window opens.
8. Click **Save**.
9. Browse to the location on your computer to save the file and click **Save**.

# 11. Reports Wizard

To create reports or run the reports wizard the ExClouds software needs to be installed.

First time users should refer to Chapter 10 before attempting to run the reports wizard.

## 11.1 Initiating the Report Wizard

The Report wizard guides you through the process of creating various reports from the ExpansE web application as described in detailed in this chapter.

*To initiate the report wizard:*

1. Click the ExClouds icon from either the desktop or the start menu.
   The ExClouds software login screen opens.

**Figure 174: ExClouds – Login Screen**

2. Enter your password and click **Login**. The default password is *admin*.
   The ExClouds main window opens with the optional reports open on the left.

**Figure 175: ExClouds – Main Window with Report Option Open**

3. Select the desired report and follow the wizard steps as described in detail in the following sections.

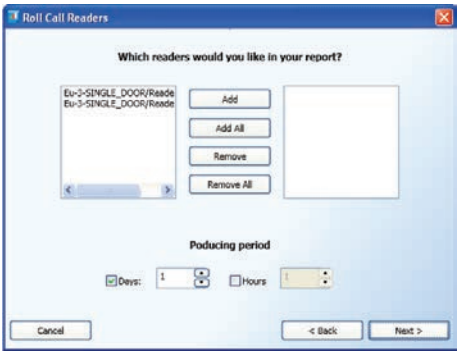
## 11.2 Creating Roll Call Reader Report

A roll call reader report generates a report showing access granted events for specific readers based on specific times.

*To create a roll call reader report:*

1. Initiate the reports wizard as described in Section 11.1.
2. Select the **Roll Call Readers Report** located under **Live Report**.
   The *Roll Call Readers* Welcome screen opens.
3. Click **Next** to start defining the report options.
   The *Parameter* screen opens.

**Figure 176: Roll Call Readers Wizard – Parameter Screen**

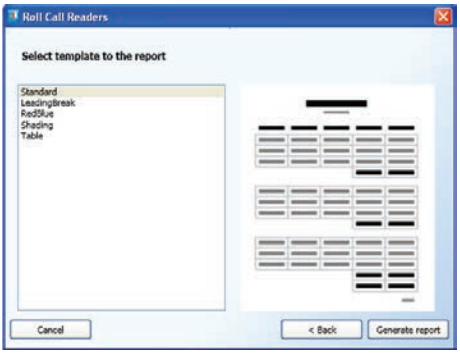



4. In the parameter screen select the readers desired for the report from the list of available readers on the left and click **Add**. You can also use the **Add All** button to select all of the readers available.

5. To remove readers from the selection list, select the reader from the list on the right and click **Remove**. Alternatively you can click the **Remove All** button to remove the entire list of readers.
6. Define the number of days you wish to view in the report by typing the number in the **Days** field or using the scroll-bar.

   Select the Hours option to define a specific number of hours, then enter the number in the **Hours** field or use the scroll-bar.
7. Click **Next** to define the look of the report in the report design template screen.

**Figure 177: Roll Call Readers Wizard – Report Design Template Screen**




8. Select the desired report template from the list of available templates.

   A preview appears on the right.
9. Click the **Generate Report** button to issue the report.

## 11.3 Creating Last Known Position Report

The last known position report creates a report showing the last valid entry for all of the users in the system for the last day.

*To create a last known position report:*

1. Initiate the reports wizard as described in Section 11.1.
2. Select the **Last Known Position Report** located under **Live Report**.

   The *Last Known Position* Welcome screen opens.
3. Click **Next** to define the look of the report in the report design template screen (see Figure 176).
4. Select the desired report template from the list of available templates.

   A preview appears on the right.
5. Click the **Generate Report** button to issue the report.

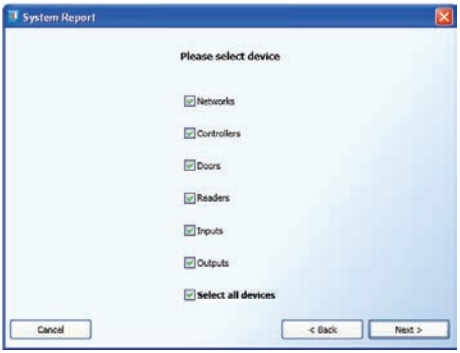
## 11.4 Creating System Report

The system report is the most detailed report available, it shows various (or all) events for selected devices based on event types and specified time frames.

*To create a system report:*

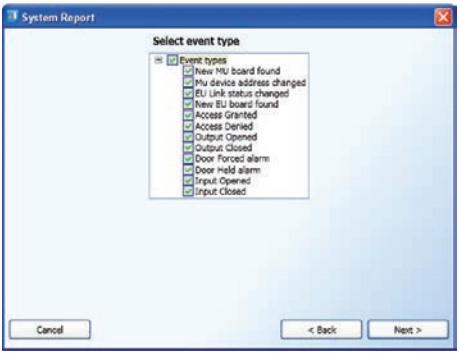
1. Initiate the reports wizard as described in Section 11.1.
2. Select the **System Report** located under **Interactive Report**.
   The *System Report* Welcome screen opens.
3. Click **Next** to start defining the report options.
   The *Device Selection screen* opens.

**Figure 178: System Report Wizard – Device Selection Screen**




4. Select the devices you wish to include in the report by selecting or clearing the box adjacent to each of the available devices. Alternatively, you can select the *Select all devices* checkbox.
5. Click **Next**.
   The *Select event type screen* opens.

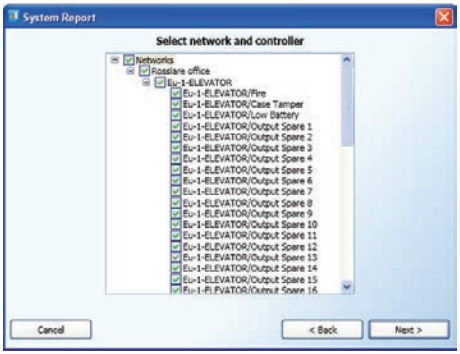
**Figure 179: System Report Wizard – Select Event Type Screen**



6. Select the events you wish to include in the report by selecting or clearing the box adjacent to each of the available events.
7. Click **Next**.

   The *Select Network and Controller* screen opens.

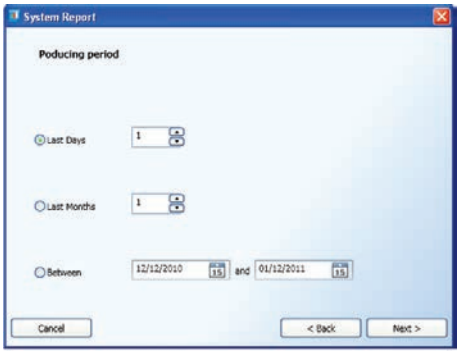
**Figure 180: System Report Wizard – Network & Controller Selection**




8. Select the networks and/or controllers you wish to include in the report by selecting or clearing the box adjacent to each of the available controllers or networks.
9. Click **Next** to continue.

   The *Producing period screen* opens.

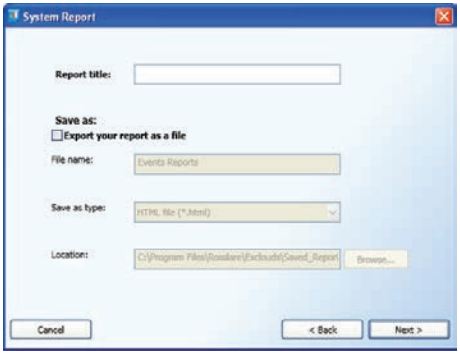
**Figure 181: System Report Wizard – Producing Period Screen**




10. Select the desired time frame for the report by either selecting a number of days, the number of months or a time frame based on actual dates.
11. Click **Next** to continue.

    The Save r*eport screen* opens.

**Figure 182: System Report Wizard – Report Save Option Screen**




12. In the **Report title** field, enter a name for the report.
13. To save the report as a file:
    a. Select the **Export your report as file** checkbox.
    b. In **File name**, enter a file name.
    c. In **Save as type,** select the format in which you wish to save the file.
    d. In **Location**, use the **Browse** button to enter the path where you would like to save the file.
14. Click **Next**.
15. In the report design template screen, define the look of the report (see Figure 176).
16. Select the desired report template from the list of available templates; a preview appears on the right.
17. Click the **Generate Report** button to issue the report.

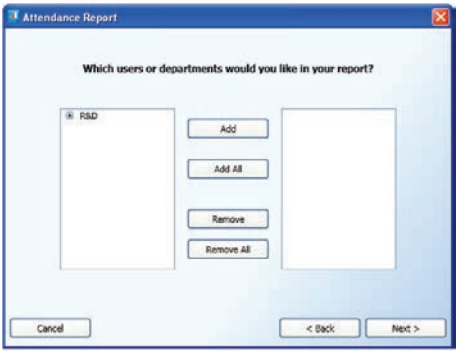
## 11.5 Creating an Attendance Report

The attendance report is the most commonly report used; it allows the creation of time & attendance reports defined by readers, users and specific time frames.

*To create an attendance report:*

1. Initiate the reports wizard as described in Section 11.1.
2. Select the **Attendance Report** located under **Interactive Report**.
   The *Attendance Report* Welcome screen opens.
3. Click **Next** to start defining the report options.
   The *User Selection Screen* opens

**Figure 183: Attendance Report Wizard – User Selection Screen**



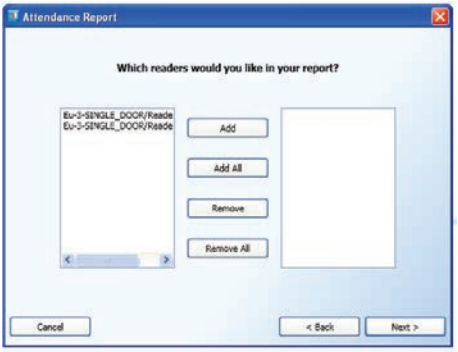

4. In the *User Selection* screen, select the departments or specific users for the attendance report from the list of available departments and users on the left and click **Add**. You can also use the **Add All** button to select all of the users.

   To remove users or entire departments from the selection list, select a line from the list on the right, and click **Remove**. Alternatively you can click the **Remove All** button to remove the entire list of users.

5. Click **Next** to continue.

   The *Reader Selection Screen* opens.

**Figure 184: Attendance Report Wizard – Reader Selection Screen**



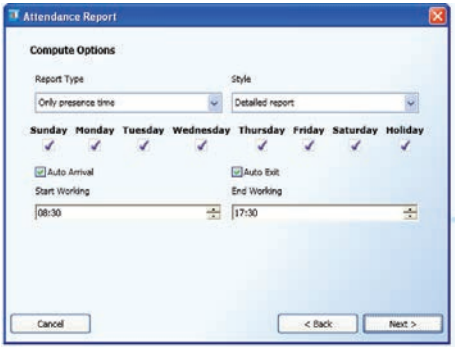

6. Select the readers associated with the desired report from the list of available readers on the left and click **Add**. You can also use the **Add All** button to select all of the readers available.

   To remove readers from the selection list, select the reader from the list on the right, and click **Remove**. Alternatively you can click the **Remove All** button to remove the entire list of readers.

7. Click **Next** to continue.

   The *Attendance Report screen* opens.

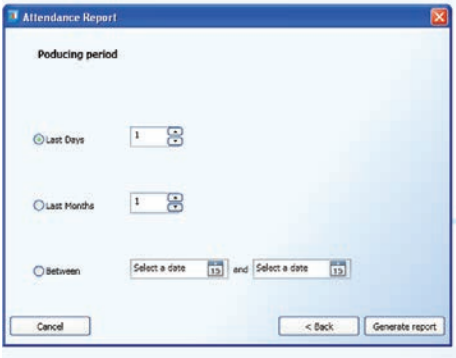
**Figure 185: Attendance Report Wizard – T&A Options Screen**




8. Define the various parameters for the time & attendance report.
   a. Select the **Report Type**, the report **Style**, and the relevant days for the report.
   b. Define the normal working hours using the **Start Working** and **End Working** select boxes. You can also define Automatic entry and exit in case of missing information by selecting the **Auto Arrival** and **Auto Exit** checkboxes respectively.
9. Click **Next** to continue.

   The *Producing period* screen opens.

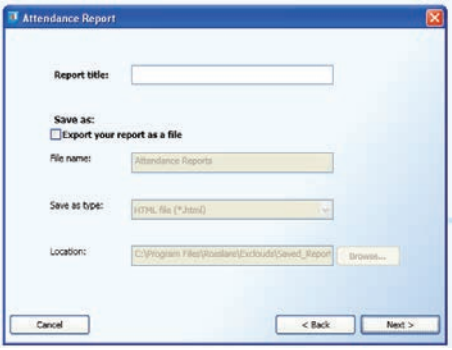
**Figure 186: Attendance Report Wizard – Producing Period Screen**




10. Select the desired time frame for the report by either selecting a number of days, the number of months or a time frame based on actual dates.
11. Click **Next** to continue.

    The *Report save option Screen* opens.

**Figure 187: Attendance Report Wizard – Report Save Option Screen**




12. In the **Report title** field, enter a name for the report for easier location and retrieval.
13. To save the report as a file, select the **Export your report as file** option.
    a. Give the file a name by typing it into the **File name:** field.
    b. Select the type of file you wish to save from the **Save as type:** file option list.
    c. Enter or **Browse** the file **Location**.
14. Click **Next** to define the look of the report in the report design template screen (see Figure 176).
15. Select the desired report template from the list of available templates.

    A preview appears on the right.
16. Click the **Generate Report** button to issue the report.

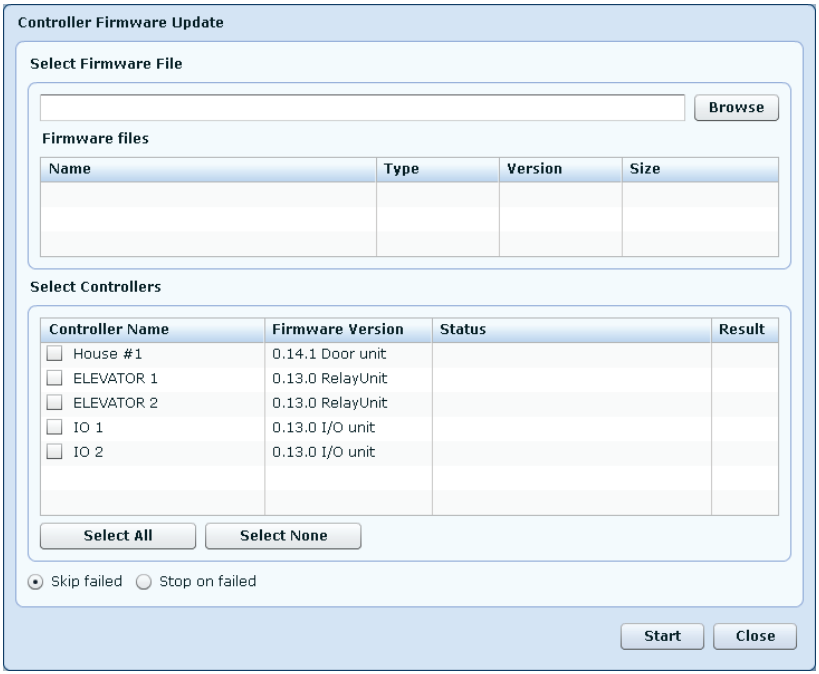
# 12. Firmware Update

You can update the firmware of various EUs as needed.

*To update firmware:*

1. Click Tools>Update Firmware.
   The *Update Firmware* window opens.

**Figure 188: Controller Firmware Update Window**

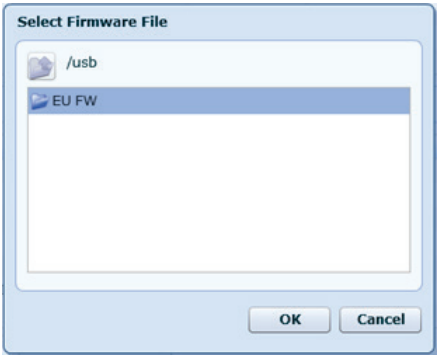



2. Click **Browse** to view the USB stick folder with the firmware files for update.

Note

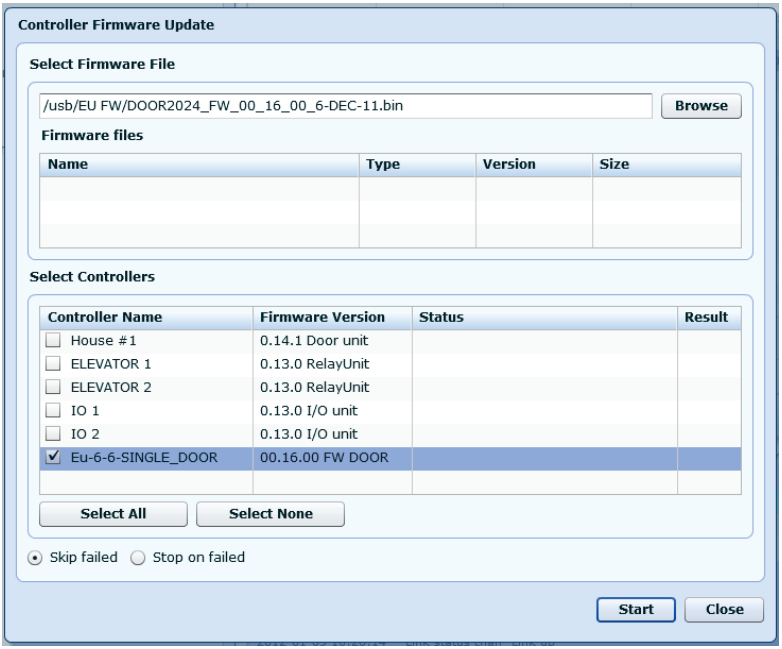
The NTFS file system format is not supported.

**Figure 189: USB Stick Files for Firmware Update**




3. Browse and select one of the three firmware updated files (door, input/output, and elevator).
4. Select the relevant EU that you wish to upgrade.

**Figure 190: Selecting EU to Update Firmware**




Note

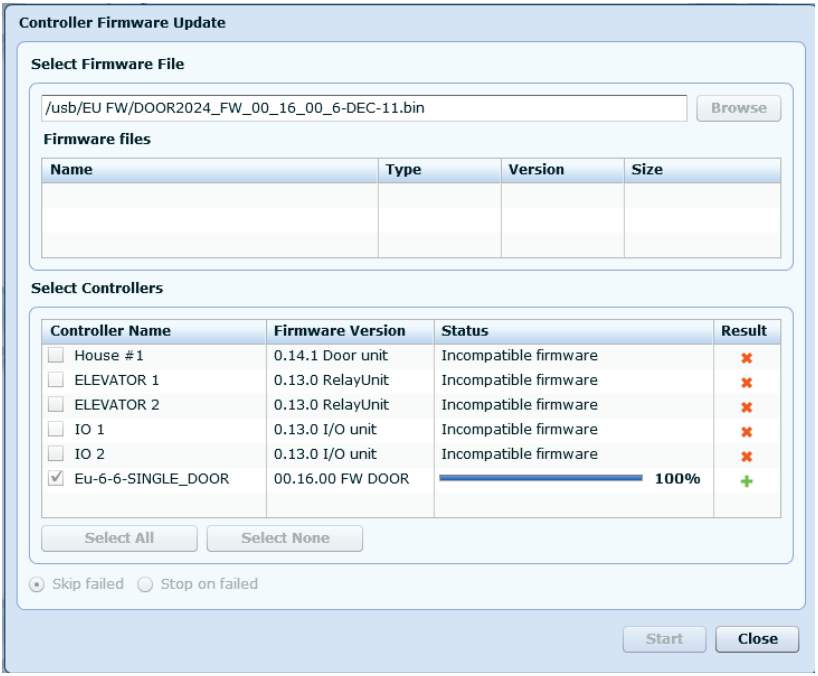
You can only update an EU with Version 00.16.00 or higher.

5. Click **Start** to begin the update process.

Note

Once you choose which type of firmware to update, you should choose only EUs of that type; otherwise, you receive an error message when trying to begin the update. You can continue with the update but an "X" appears next to those EUs that were not updated (Figure 190).

**Figure 191: Firmware Update Progress**




When the update completes successfully, a confirmation window opens.

6. Click **OK**.

# A. Example of Wiring an Elevator Unit

**Figure 192: Wiring Diagram of 4-Floor Elevator to EXP-2016**

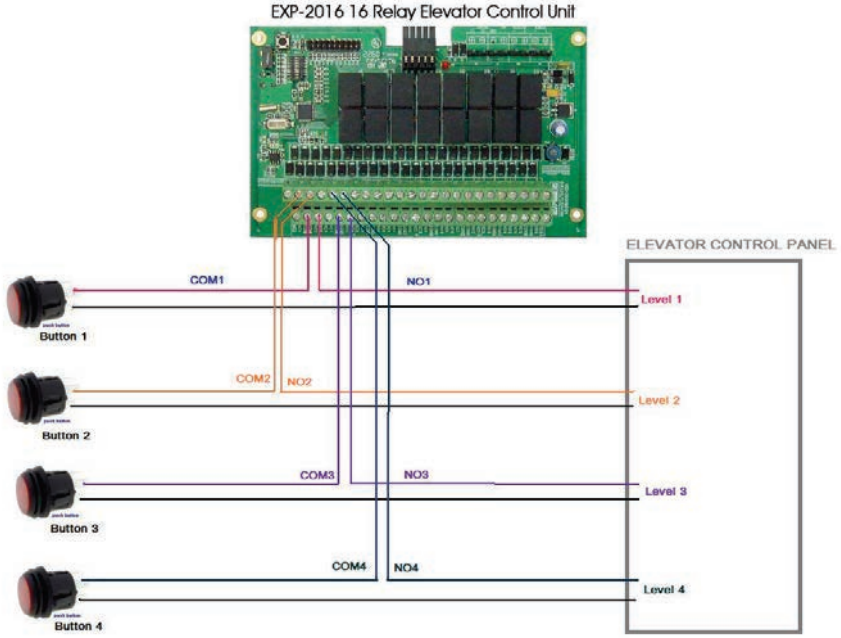
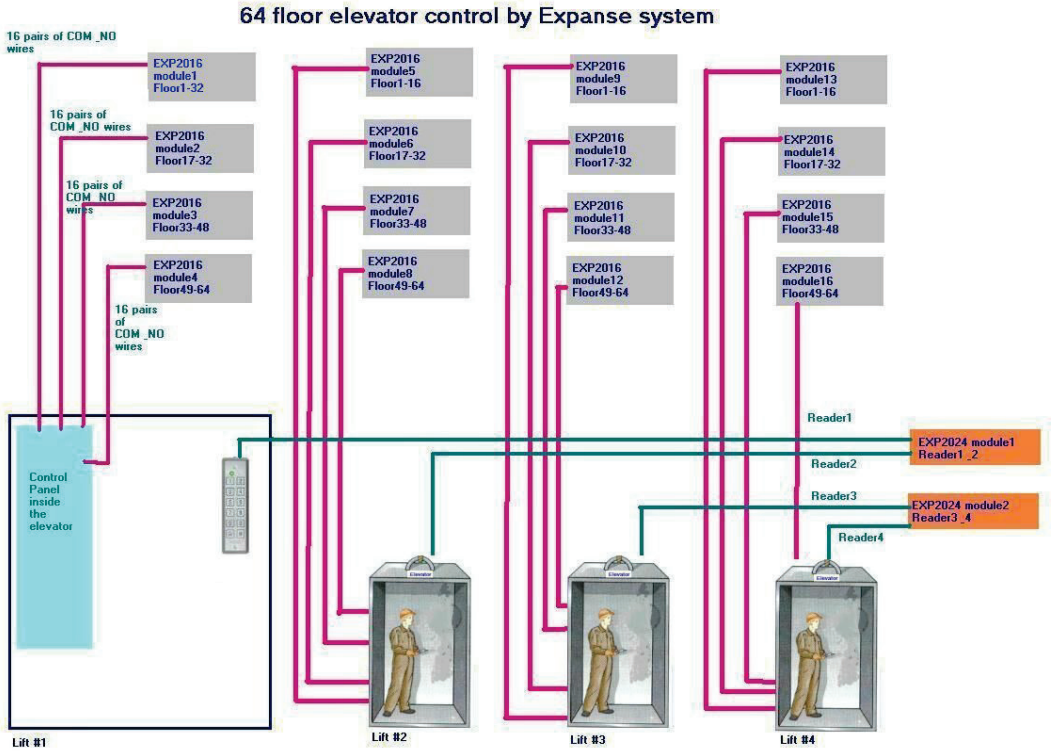


Figure 193: Connection Diagram of Four 64-Floor Elevators



# B. Limited Warranty

ROSSLARE ENTERPRISES LIMITED (ROSSLARE) TWO-YEAR LIMITED WARRANTY is applicable worldwide. This warranty supersedes any other warranty. ROSSLARE'S TWO-YEAR LIMITED WARRANTY is subject to the following conditions:

#### WARRANTY

Warranty of ROSSLARE'S products extends to the original purchaser (Customer) of the ROSSLARE product and is not transferable.

#### PRODUCTS COVERED BY THIS WARRANTY AND DURATION

ROSSLARE ENTERPRISES LTD. AND/OR SUBSIDIARIES (ROSSLARE) warrants that the EXPANSE Access Control System to be free from defects in materials and assembly in the course of normal use and service. The warranty period commences with the date of shipment to the original purchaser and extends for a period of 2 years (24 months).

#### WARRANTY REMEDY COVERAGE

In the event of a breach of warranty, ROSSLARE will credit Customer with the price of the Product paid by Customer, provided that the warranty claim is delivered to ROSSLARE by the Customer during the warranty period in accordance with the terms of this warranty. Unless otherwise requested by a ROSSLARE representative, return of the failed product(s) is not immediately required.

If ROSSLARE has not contacted the Customer within a sixty (60) day holding period following the delivery of the warranty claim, Customer will not be required to return the failed product(s). All returned Product(s), as may be requested at ROSSLARE'S sole discretion, shall become the property of ROSSLARE.

To exercise the warranty, the user must contact ROSSLARE Enterprises Ltd. to obtain an RMA number after which, the product must be returned to the Manufacturer freight prepaid and insured.

In the event ROSSLARE chooses to perform a product evaluation within the sixty (60) day holding period and no defect is found, a minimum US$ 50.00 or equivalent charge will be applied to each Product for labor required in the evaluation.

ROSSLARE will repair or replace, at its discretion, any product that under normal conditions of use and service proves to be defective in material or workmanship. No charge will be applied for labor or parts with respect to defects covered by this warranty, provided that the work is done by ROSSLARE or a ROSSLARE authorized service center.

### EXCLUSIONS AND LIMITATIONS

ROSSLARE shall not be responsible or liable for any damage or loss resulting from the operation or performance of any Product or any systems in which a Product is incorporated. This warranty shall not extend to any ancillary equipment not furnished by ROSSLARE, which is attached to or used in conjunction with a Product, nor to any Product that is used with any ancillary equipment, which is not furnished by ROSSLARE.

This warranty does not cover expenses incurred in the transportation, freight cost to the repair center, removal or reinstallation of the product, whether or not proven defective.

Specifically excluded from this warranty are any failures resulting from Customer's improper testing, operation, installation, or damage resulting from use of the Product in other than its normal and customary manner, or any maintenance, modification, alteration, or adjustment or any type of abuse, neglect, accident, misuse, improper operation, normal wear, defects or damage due to lightning or other electrical discharge. This warranty does not cover repair or replacement where normal use has exhausted the life of a part or instrument, or any modification or abuse of, or tampering with, the Product if Product disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection and testing to verify any warranty claim.

ROSSLARE does not warrant the installation, maintenance, or service of the Product. Service life of the product is dependent upon the care it receives and the conditions under which it has to operate.

In no event shall ROSSLARE be liable for incidental or consequential damages.

### LIMITED WARRANTY TERMS

THIS WARRANTY SETS FORTH THE FULL EXTENT OF ROSSLARE'S WARRANTY.

THE TERMS OF THIS WARRANTY MAY NOT BE VARIED BY ANY PERSON, WHETHER OR NOT PURPORTING TO REPRESENT OR ACT ON BEHALF OF ROSSLARE.

THIS LIMITED WARRANTY IS PROVIDED IN LIEU OF ALL OTHER WARRANTIES. ALL OTHER WARRANTIES EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE SPECIFICALLY EXCLUDED.

IN NO EVENT SHALL ROSSLARE BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, OR FOR ANY OTHER INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF USE, LOSS OF TIME, COMMERCIAL LOSS, INCONVENIENCE, AND LOSS OF PROFITS, ARISING OUT OF THE INSTALLATION, USE, OR INABILITY TO USE SUCH PRODUCT, TO THE FULLEST EXTENT THAT ANY SUCH LOSS OR DAMAGE MAY BE DISCLAIMED BY LAW.

THIS WARRANTY SHALL BECOME NULL AND VOID IN THE EVENT OF A VIOLATION OF THE PROVISIONS OF THIS LIMITED WARRANTY.

## Asia Pacific, Middle East, Africa

Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
support.apac@rosslaresecurity.com

## United States and Canada

Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

## Europe

Rosslare Israel Ltd.
Rosh HaAyin, Israel
Tel: +972 3 938-6838
Fax: +972 3 938-6830
support.eu@rosslaresecurity.com

## Latin America

Rosslare Latin America
Buenos Aires, Argentina
support.la@rosslaresecurity.com

## China

Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86 755 8610 6842
Fax: +86 755 8610 6101
support.cn@rosslaresecurity.com


0706-0960230+00

ROSSLARE
SECURITY PRODUCTS
www.rosslaresecurity.com

ROSSLARE SECURITY PRODUCTS